January 2015

An Approach to Near Field Data Selection in Radio Frequency Identification

Robert D. Winkworth
Purdue University

Graduate School Form 30
Updated 1/15/2015

PURDUE UNIVERSITY
GRADUATE SCHOOL
Thesis/Dissertation Acceptance

This is to certify that the thesis/dissertation prepared

By Robert D. Winkworth

Entitled

An Approach to Near Field Data Selection in Radio Frequency Identification

For the degree of Doctor of Philosophy

Is approved by the final examining committee:

Michael J. Dyrenfurth
Chair

Eugene H. Spafford

Kathryn A. Newton

Marcus K. Rogers

To the best of my knowledge and as understood by the student in the Thesis/Dissertation Agreement, Publication Delay, and Certification Disclaimer (Graduate School Form 32), this thesis/dissertation adheres to the provisions of Purdue University's "Policy of Integrity in Research" and the use of copyright material.

Approved by Major Professor(s): Michael J. Dyrenfurth

Approved by: Kathryne A. Newton 10/7/2015

Head of the Departmental Graduate Program Date

AN APPROACH TO NEAR FIELD DATA SELECTION IN RADIO FREQUENCY IDENTIFICATION

A Dissertation

Submitted to the Faculty

of

Purdue University

by

Robert D. Winkworth

In Partial Fulfillment of the

Requirements for the Degree

of

Doctor of Philosophy

December 2015

Purdue University

West Lafayette, Indiana

ACKNOWLEDGEMENTS

Research was made possible by support from sponsors including the Center for Education and Research in Information Assurance and Security. Recognized as the nation's preeminent facility of its kind, CERIAS continues to empower graduates including the author with computing resources, lab space, library collections, funding, and above all, the opportunity to collaborate with renowned industry and academic experts.

To have the center's founder as a member of the doctoral committee reviewing this dissertation is a distinct honor.

TABLE OF CONTENTS

Page

Page

Page

LIST OF TABLES

LIST OF FIGURES

GLOSSARY

Unless used otherwise in context, terms shall be defined as follows. Those definitions that conform to established industry or academic sources are drawn from the dictionaries cited.

Active Tag:	Tags that use batteries as a partial or complete source of power to boost the effective operating range of the tag and to offer additional features over passive tags (*RFID Glossary*, n.d.).
AIDC:	Automatic Identification and Data Capture - technologies including bar codes, smart media, biometrics, and RFID (*RFID Glossary*, n.d.).
Antenna:	That part of a transmitting or receiving system that is designed to radiate or to receive electromagnetic waves (*Authoritative Dictionary of IEEE Standards Terms, Seventh Edition*, 2007).
Backscatter:	A method of communication between passive tags and readers. RFID tags using backscatter technology reflect back to the reader radio waves from a reader, usually at the same carrier frequency. The reflected signal is modulated to transmit data (*Glossary of RFID Terms*, 2014).

Band:	Range of frequency between two defined limits (*Authoritative Dictionary of IEEE Standards Terms, Seventh Edition*, 2007).
Capacitive:	An electromagnetic signal transmission coupling mode that occurs in the near field from an antenna that preferentially emits electric field over magnetic field such as an electric dipole antenna (*Authoritative Dictionary of IEEE Standards Terms, Seventh Edition*, 2007).
Coupling:	The association of two or more circuits or systems in such a way that power or signal information may be transferred from one to another (*Authoritative Dictionary of IEEE Standards Terms, Seventh Edition*, 2007).
Data Field:	An ID card's smallest component of data entry and storage.
Die:	The silicon block onto which circuits have been etched to create a microchip (*Glossary of RFID Terms*, 2014).
Dipole:	A linear radiator, usually fed in the center, producing a maximum of radiation in the plane normal to its axis. The length specified is the overall length. Any one of a class of antennas producing the radiation pattern approximating that of an elementary electric dipole (*Authoritative Dictionary of IEEE Standards Terms, Seventh Edition*, 2007).
Driven Element:	A radiating element coupled directly to the feed line of an antenna (*Authoritative Dictionary of IEEE Standards Terms, Seventh Edition*, 2007).

Duty cycle:	The percentage of time the reader is emitting energy (*Glossary of RFID Terms*, 2014).
Dwell Time:	The time a transit unit spends at a station or stop, measured as the interval between its stopping and starting (*Authoritative Dictionary of IEEE Standards Terms, Seventh Edition*, 2007).
Excitation:	Charging of a passive tag by transmitting RF energy from a reader, to activate the tag and enable response (*Glossary of RFID Terms*, 2014).
Far Field:	A region in which the RF power delivered from an antenna decreases by the square of its distance from the antenna. A region where coupling is primarily electromagnetic (*Glossary of RFID Terms*, 2014).
Feed Line:	A transmission line interconnecting an antenna and a transmitter or receiver or both (*Authoritative Dictionary of IEEE Standards Terms, Seventh Edition*, 2007).
Frequency:	The number of periods of an oscillation or wave occurring in unit time of a periodic quantity, in which time is the independent variable (*Authoritative Dictionary of IEEE Standards Terms, Seventh Edition*,2007).
Half Duplex:	A communication channel capable of transmitting data in both directions, but not simultaneously (*Glossary of RFID Terms*, 2014).

Hashing:	A process of applying a mathematical algorithm against a set of data to produce a numeric value (a 'hash value') that represents the data (*Glossary of Common Cybersecurity Terminology*, n.d.).
Induction:	The process of generating time-varying voltages and/or currents in otherwise un-energized conductive objects or electric circuits by the influence of the time-varying electric and/or magnetic fields (*Authoritative Dictionary of IEEE Standards Terms, Seventh Edition*, 2007).
Insulation:	A material that has electrical insulating properties and is used to separate parts that have different voltages (*Authoritative Dictionary of IEEE Standards Terms, Seventh Edition*, 2007).
Isotropic:	Having the same properties in all directions (*Authoritative Dictionary of IEEE Standards Terms, Seventh Edition*, 2007).
Key:	The numerical value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification (*Glossary of Common Cybersecurity Terminology*, n.d.).
Lobe:	A portion of the antenna directional pattern bounded by one or two cones of nulls (*Authoritative Dictionary of IEEE Standards Terms, Seventh Edition*, 2007).

Microcontroller:	A processing device that has the capability needed to receive data from external devices, analog or digital or both, process the data according to preset algorithms or special computing techniques or both, and then provide the results to external devices for the end purpose of controlling the process (*Authoritative Dictionary of IEEE Standards Terms, Seventh Edition*, 2007).
Modulation:	Alteration of a wave characteristic so that it may serve as a carrier of information.
Near Field:	The region of the field of an antenna between the reactive near field region and the far field region wherein radiation fields predominate and wherein the angular field distribution is dependent upon distance from the antenna (*Authoritative Dictionary of IEEE Standards Terms, Seventh Edition*, 2007).
Null:	The direction between radiation lobes where the signal drops to a minimum. In general, a null is any portion of the pattern where the signal level is less than 10% of the RMS of the pattern (*Authoritative Dictionary of IEEE Standards Terms, Seventh Edition*, 2007).
Parasitic element:	A radiating element that is not connected to the feed lines of an antenna and that materially affects the radiation pattern or impedance of an antenna, or both (*Authoritative Dictionary of IEEE Standards Terms, Seventh Edition*, 2007).

Passive Tag:	The most common RFID tags, in which a reader transmits an energy field that "wakes up" the tag and provides the power for the tag to operate (*RFID Glossary*, n.d.).
Permittivity:	The ratio of electric flux density D to electric field strength E (*Authoritative Dictionary of IEEE Standards Terms, Seventh Edition*, 2007).
Polarization:	That property of periodic electric or magnetic field describing the figure traced over one cycle by the extremity of the field vector at a fixed location in space (*Authoritative Dictionary of IEEE Standards Terms, Seventh Edition*, 2007).
Radome:	A cover, usually intended for protecting an antenna from the effects of its physical environment without degrading its electrical performance (*Authoritative Dictionary of IEEE Standards Terms, Seventh Edition*, 2007).
Reader:	A wireless device that supplies modulated RF energy to passive tags and accepts a signal in reply, for the purpose of interrogating the tag for information.
RF Field:	RF electrical and magnetic fields emitted from antenna/transmitter arrays (*Authoritative Dictionary of IEEE Standards Terms, Seventh Edition*, 2007).
Singulation:	A means by which an RFID reader identifies a tag with a specific serial number from a number of tags in its field, usually by traversing a tree of serial number segments.

Transponder:	A tag incorporating a microchip and antenna that can be programmed with information to identify entities and transmit that information to a receiver (*RFID Glossary*, n.d.).
Tuned:	Adjusted for responsiveness to a target frequency.
Tuple:	A data type similar to a list, containing a set of values in which the same element may appear more than once.
Wavelength:	The distance along the direction of propagation of a periodic wave between two successive points where, at a given time, the phase is the same (*Authoritative Dictionary of IEEE Standards Terms, Seventh Edition*, 2007).

ABSTRACT

Winkworth, Robert D. Ph.D., Purdue University, December 2015. An Approach to Near Field Data Selection in Radio Frequency Identification. Major Professor: Michael J. Dyrenfurth.

Personal identification is needed in many civil activities, and the common identification cards, such as a driver's license, have become the standard document de facto. Radio frequency identification has complicated this matter. Unlike their printed predecessors, contemporary RFID cards lack a practical way for users to control access to their individual fields of data. This leaves them more available to unauthorized parties, and more prone to abuse. Here, then was undertaken a means to test a novel RFID card technology that allows overlays to be used for reliable, reversible data access settings. Similar to other proposed switching mechanisms, it offers advantages that may greatly improve outcomes. RFID use is increasing in identity documents such as drivers' licenses and passports, and with it concern over the theft of personal information, which can enable unauthorized tracking or fraud. Effort put into designing a strong foundation technology now may allow for widespread development on them later.

In this dissertation, such a technology was designed and constructed, to drive the central thesis that selective detuning could serve as a feasible, reliable mechanism. The concept had been illustrated effective in limiting access to all fields simultaneously before, and was here effective in limiting access to specific fields selectively. A novel card was produced in familiar dimensions, with an intuitive interface by which users may conceal the visible print of the card to conceal the wireless emissions it allows. A discussion was included of similar technologies, involving capacitive switching, that could further improve the outcomes if such a product were put to large-scale commercial fabrication.

The card prototype was put to a battery of laboratory tests to measure the degree of independence between data fields and the reliability of the switching mechanism when used under realistically variable coverage, demonstrating statistically consistent performance in both. The success rate of RFID card read operations, which are already greater than 99.9%, were exceeded by the success rate of selection using the featured technology. With controls in place for the most influential factors related to card readability (namely the distance from the reader antennas and the orientation of the card antenna with respect to them), the card was shown to completely resist data acquisition from unauthorized fields while allowing unimpeded access to authorized fields, even after thousands of varied attempts. The effect was proven to be temporary and reversible. User intervention allowed for the switching to occur in a matter of seconds by sliding a conductive sleeve or applying tape to regions of the card.

Strategies for widespread implementation were discussed, emphasizing factors that included cost, durability, size, simplicity, and familiarity, all of which arise in card management decisions for common state and national identification such as a driver's license. The relationship between the card and external database systems was detailed, as no such identification document could function in isolation. A practical solution involving it will include details of how multiple fields will be written to the card and separated sufficiently in external databases so as to allow for user-directed selection of data field disclosure. Opportunities for implementation in corporate and academic environments were discussed, along with the ways in which this technology could invite further investigation.

CHAPTER 1. INTRODUCTION

1.1 Background

The ability to uniquely identify people is vital to contemporary life, defining not only the limits of privilege or affiliation, but also the very relationship between citizen and state (Clement, McPhail, Smith, & Ferenbok, 2012). For long, the most common method of formal identification in the United States has been the driver's license or similar state-issued identification card, but with the advent of Radio Frequency Identification--RFID--there is new interest in replacing these methods with devices capable of wirelessly determining a user's identity using small, programmable chips with onboard signaling components (Marquardt, Taylor, Villar, & Greenberg, 2010). Such chips have been used widely in manufacturing, distribution, and sales applications, and then began to appear in forms of government-issued personal identification such as driver's licenses and passports (Gertz, 2008). The technology employed makes possible greater efficiency and greater flexibility than was possible with printed, optical, and magnetic cards; but it does not currently allow for the same protections against unauthorized disclosure of personal information (Phillips, Karygiannis, & Kuhn, 2005).

A driver's license and most other such cards contain a photograph of the intended user and several fields of information such as name, age, gender, etc. Until now, if a user was called upon to provide proof of identity using a photographic ID card, it was a minor matter to withhold fields as desired. Proof of the user's name with respect to the photograph, for example, could be made by displaying or optically scanning a copy of the card, exposing the name and photograph, but obscuring the remaining fields with an overlay. Proof of age with respect to name could be made likewise by exposing these two

fields while obscuring the rest, and many other combinations are possible. The user retains control over the extent of the disclosure in these cases; no more or less is revealed than is necessary to perform the intended test (Clement et al., 2012).

If, however, the printed card is replaced with the type of wireless chip now used in identification documents such as passports, there is no such means for selection. Provided normal operating conditions, the chip's entire contents are disclosed to any authenticated RFID reader within range (Mahmood & Al-Hamdani, 2011). This means that, for example, an airport traveler who intended to present one passport page would be forced to share his entire travel history whenever he so much as opened his passport. Likewise, a consumer that wished to prove his name or age would also be forced to share any additional information on the RFID card used, without any forthright means to limit it.

As with other forms of identification, RFID needs, for a successful deployment, to take into account who and what retains custody of the information, what mechanism is used to release it, who shall be responsible for the decision, and how much information is really needed to complete the desired transaction. Printed identification cards used in combination with overlays and photocopying devices provide a means of limiting disclosure to only those portions of the card so needed. The number and combination of portions may be chosen in each transaction independently. When print gives way to automatic mechanisms, this choice may be lost. RFID is a prime example.

Radio-frequency identification cards complicate this matter in several ways. The fields are no longer visible on the card itself, and can no longer be obscured independently. The most a cardholder was originally able to do to prevent its information from being read (without causing physical damage) was shielding the entire card, or staying so far away from electronic readers as to be considered out of range.

One of the earliest measures taken to curb the threat of unauthorized scanning was to employ RF-opaque covers that could be used over the RFID document. US passports were among these (Lawson, 2008). A variety of these covers have been tested in this study's lab, and found to have an actual effectiveness against read attempts that does not always agree with advertised claims. Nonetheless, they do illustrate an important fact: the RFID component--specifically the antenna--is degraded noticeably when conductive materials are too close. This occurs both because a sufficiently conductive enclosure has a shielding effect on electromagnetic radiation, and because even open conductors of sufficient length will still cause detuning of the antenna, reducing its performance on the intended frequency band. Federal and state officials recommend the use of such covers on RFID passports and driver's license cards (Lewan, 2009). What they would need to provide granular selection, however, is a way to make opaque only certain, private data fields, while allowing for access to the rest. This is a flexibility not currently available in federal or state RFID models (Nogueira & Greis, 2009).

What the research of this dissertation demonstrated is a model that allows access to the fields to be toggled independently, using visible, intuitive methods and familiar card geometry, the sort found in current deployments to large state populations. RFID has been deployed in a number of cases where it had been billed as introducing new security, but actually introduced weaknesses, because it failed to adhere to the principles above (Lawson, 2008). What makes for an effective solution is not a technology alone, but the principles, however enacted. RFID provides a means to enact them readily, and is attractive not only because the devices are powerful, but also because they produce a palpable effect. Users have been shown more likely to adopt security mechanisms that make them feel safer rather than those that produce the same effects without any indicators that users can sense (Schneier, 2008).

As a practical matter, not all ID users are concerned about the unnecessary disclosure of personal information. For them, losing a protection that they were not using anyway might not draw complaint. Nonetheless, when one technology, such as RFID, is

introduced as the replacement to another, such as printed cards, there arises cause for concern if the successor offers a lower functionality, or a higher vulnerability to abuse. Users might question whether it is, in all regards, an improvement over the current technology. They might discover, only when the new is established widely, that the old had offered unique utility, through features that cannot be easily reintroduced. This outcome seems likely in light of the common public lack of awareness of the security and privacy risks associated with RFID (Marqhardt et al., 2010).

Among the concerns that are known to arise among users is how identifying documents are used to commit acts of impersonation and fraud (Ramos, Scott, Lloyd, O'Leary, & Waldo, 2009). The popular term "identity theft" could be better phrased. Identity is not what is being taken in such cases; information is being taken, and used to misrepresent identity. Information need not be deleted from its original source, either, so rather than describing it as a theft, it might be more suitable to describe it as unauthorized access to personal information, or the unauthorized use of it (Abdullah, 2004). The real problem behind the abuses done with the information is that it is possible to conduct transactions using identifying information that is not legitimate. This is a matter fundamental to identification using any medium, but becomes particularly relevant when wireless technology is involved, with transactions that are both invisible and also able to happen without the user (or abuser) ever laying hand upon the ID document.

More than a few influential participants in the RFID industry have expressed concern over the decline in user control that comes with the new identification devices. For example, the head of wireless technology at Siemens has been an advocate of RFID for some time, noting its promise as an ID for patients in hospital, students in school, and consumers most anywhere. Yet, he tempers his enthusiasm with warnings of misuse if RFID is to be used for a widespread ID deployment. In short, "There needs to be standards put in place so the data is not abused for other purposes" (Herrmann, 2007, para. 24). As the market stands, there is available no standard that allows for user control of

which personal information is released during RFID transactions. The only control is over whether the technology is used at all.

There has been work done to address the data release issue. Functional prototypes such as those demonstrated by Marqhardt et al. had mechanisms that did not allow read operations without physical confirmation from the user (2010). This included even the capability of separating data into two classifications--low-sensitivity and high-sensitivity. It allowed the user to release one of the two sets at a time by squeezing a button built into the card (p. 2312). What was proposed for the research of the content to follow is a separation of the data fields in the identification document so the relationships among any number of them may be revealed as needed, without involving the others. Without this level of granularity, the document remains an indivisible container of data, all of which is available for any transaction with any party, and disclosure of unnecessary personal data becomes inevitable.

1.2 Problem Statement

The problem that first prompted study here was that unlike their printed predecessors, contemporary RFID cards lack a practical way for users to control access to their individual fields of data. This leaves them more available to unauthorized parties, and more prone to abuse.

1.3 Purpose of Study

The study was undertaken to test a novel RFID card technology that allows overlays to be used for reliable, reversible data access settings. It drives the central thesis that an overlay based on RF detuning is possible.

This proposed card design allows for granular user discretion over the disclosure of information units, suitable for large implementations across a diverse economic and

technological landscape. Proving it effective in a controlled environment invites work implementing the social and regulatory components of a complete personal identification solution.

1.4 Research Questions

a) Is selective detuning a feasible mechanism for independent selection of RFID card data?
b) Can a design for selective RFID detuning operate reliably enough to be practical?

1.5 Significance of Study

Every passport issued in the US incorporates RFID technology. Come the year 2017, it will be the only type accepted (Ramos et al., 2009). Public concern over "identity theft" continues to grow in the US (Abdullah, 2004), while these changes to government ID documents make unauthorized collection of information possible by methods that are faster, easier, and less noticeable than before (Lawson, 2008). Consumers who carry these documents may be tracked by the collected information, without their consent (Smith, 2010).

Effort put into designing strong foundation technologies now may allow for many decades of successful development on them later (Koscher, Juels, Kohno, & Brajkovic, 2009). This dissertation analyzes principles fundamental to effective personal identification, and offers a solution on which further development may easily follow. The central aspect addressed here is the mechanism for controlling read and write access to data fields on ID cards.

In the US, a driver's license is used far beyond the purpose of proving licensure to drive. It has also been co-opted as a general identification document, and used to open a variety of personal accounts unrelated to driving (Abdullah, 2004). The passport finds

similar uses (p. 103), offering information that may be obtained even when the holder is not in fact passing a port or even approaching a national border. The large and established base of users makes the use of these documents inviting, but superior identification technologies exist, and are tailored to the specific requirements of personal government documents (Mahmood & Al-Hamdani, 2011). While it seems quite optimistic to think that an alternative to drivers' licenses and passports will be accepted and deployed as a replacement for either, this work nonetheless has the opportunity to address concerns that are present even today, and principles of identification that belong in any such mechanism. It is offered as the basis for future decisions.

Even within the category of RFID cards, there is found more than one approach to improving hardware privacy. Methods exist for making RFID tags unique, and resilient to counterfeiting, for example, (Periaswamy, Thompson, & Di, 2011), and there are several possible hardware-based mechanisms for data field selection (Marqhardt et al., 2010). This dissertation does not represent an exhaustive demonstration of all available technologies, or assert that one should be held above all others in every context. Rather, it represents a demonstration of one attractive mechanism that has shown potential, and meets or exceeds the demands in terms of reliability, affordability, durability, etc. This can easily lead into a larger discussion of the purchasing and engineering particulars.

1.6 Delimitations

The scope of this work shall include only radio-frequency cards used for identifying personnel. Many of the principles introduced would apply also beyond cards, to include buttons, anklets, stickers, implants, and other tag packages too numerous to deal with here. This could also extend easily to a discussion of identifying products, but volumes have already been written on that topic, while certain aspects of personnel identification still appear to need attention (Heim, 2008). Note that there are distinctions drawn between the printed cards and the RFID cards that would similarly apply between the printed cards and other AIDC (machine-readable) technologies such as magnetic

stripe cards and optical pattern cards. Separate strategies would be needed to provide selective disclosure in cards using these technologies, and they cannot be addressed within scope here.

The number of personal data fields directly available on an RFID document differs according to its application. In electronic passports, multiple fields exist, and duplicate much of the information in the printed fields. In electronic driver's license cards, a single field exists containing a unique identifier that in turn is used as a primary key to a tuple of user data stored externally in a government database (Nogueira & Greis, 2009). This paper presents new technology that could be readily used in either of these documents, but would replace the current designs. Neither this nor any advancement in ID can provide a higher degree of control over how its data are used in external documents or stores, beyond curtailing its initial disclosure. The technology presented here is for direct control of the document, and not remote control functions.

RFID is separate from biometric technology, but the two are frequently deployed together. If care is not exercised, the former can greatly weaken the security of the latter. (Williams, 2009). The research presented here operates from the standpoint that whatever biometric features might be included in an RFID deployment were collected and incorporated appropriately into the card in question before its examination began. A vital function of the card, then, is to see them safeguarded, and disclosed only when and where desired. One security researcher successfully forged an RFID card that would report him as Elvis Presley to electronic readers (Timmer, 2008). Stunts such as these cannot be prevented by selective disclosure. They require separate measures, which might be as simple as keeping a human attendant with good vision involved in the process, rather than allowing full automation with no attendant (Timmer, 2008).

The work presented here is for card technology carried in hand, pocket, purse, etc., and should not be construed to apply for RFID documents small enough to be carried inside a living user. Implants face particular barriers to widespread adoption, as they

come under greater legislative scrutiny (Greenblatt, 2010). Even before the discussion turns to the health concerns surrounding implantable devices, the very thought that they could become popular enough to be mentioned in employment requirements is enough to draw firm resistance from state representatives. Several states have passed legislation strictly curtailing involuntary RFID implants, anticipating possible abuses from employers and insurance companies (Kunkle & Helderman, 2010). Though guided by some principles that are not scientifically correct, these government figures have made it unlikely that a national standard for implanted identification could ever be imposed in the US. This matter shall not be explored further here.

Standards of identification used in countries other than the US are beyond scope of this paper as well, even though the findings from it might still prove applicable to what other countries need. State identification cards carry similar information in many countries, and share similar cost and durability requirements, so there is likely to be opportunity here for further regional study. The technology of ID has applications that are inviting in many national contexts; consider (Qaiser & Khan, 2006) or (Lehman, 2012). Points regarding identification outside the US shall be included where they illustrate general principles, but are distinguished from points of policy or government.

This paper presents a prototype RFID device and the tests of its ability to select for and against data disclosure. A mechanism is engineered and used to distinguish data fields with a metallic overlay. In later reproductions of this effect, it shall be considered beyond scope to include variation that might occur resulting from

- Manufacturing defects
- Lack of metal purity standards
- Intentional tampering and misuse
- Public RF sources in excess of FCC limits

The tests concern only the hardware mechanism and electrical principles of the prototype. No testing is presented here of the materials commercial suppliers might later

offer or the automation process they might introduce to scale the manufacturing from the small quantity of prototype units up to a large quantity of commercial production units.

The detuning effects on high frequency tags are known to vary according to the antenna geometry used. They show predictably greater variation than is found in a card specifically designed for capacitive switching. This experiment and the numerical analyses to follow serve as an illustration of what is possible in mechanisms of selective disclosure, presented with the hope that others explore and optimize them to suit individual needs.

In brief, the mechanism at work in a capacitive design is slightly different than the detuning effect used here. It employs sensors that measure the overlay's permittivity--its willingness to allow an electric field to form through it. Inputs from these sensors are processed by the card's control circuitry during an attempted read operation, and instruct it to remain silent if the overlay is in place. In a laboratory setting, the effect on data field selection is the same for cards in both of these two categories, and for purposes of this experiment, either will do to demonstrate the principle. For future production, though, the capacitive design requires fewer parts, greater engineering flexibility, and even higher reliability when it comes to surface area of overlay coverage, so it represents a good opportunity for further study.

1.7 Research Flow

The focus of this research could have been drawn to any one of several problems currently challenging radiofrequency identification, so it might be worthwhile to briefly describe the progression from general topics down into the specific factors tested:

The work presented here begins with the problem of controlling access to card regions. From this leads a path suitable for each of the two research questions, a & b. Each of these has a separate hypothesis, which was tested by its own suited methods. The collected data were analyzed separately according to the numerical tests chosen for the hypothesis. The result for each of the tests was recorded. The two results led to their respective conclusions, and to recommendations on selective detuning. From this come the recommendations for deployment of a personnel identification technology based on selective detuning, and recommendations for continuing research in it.

It is important to remember that while these two separate tracks of experimental testing are described here in sections of their own, they form the two vital supports of the final, unifying summary of the model and its prototype. Ultimately, this is research into the model. It was tested according to two crucial questions, and found effective. Only because of this was it seen as worthy of further consideration, and only because of this is it offered as one proposal for solving the stated problem of lost granular control over data field access in ID cards.

CHAPTER 2. LITERATURE REVIEW

2.1 Methods Used

It becomes clear early in an investigation of the literature that the RFID industry leaves many opportunities for security research and improvement. Entire volumes have been written on applications specific to warehousing, transportation, sales, and overall supply chain management, for example. Security in these matters is largely a matter of sustaining business and preventing sabotage, so most of its literature is not directly applicable to citizen identification.

Even when limited to personal devices worn and carried, the body of knowledge is huge, and increased even as this review proceeded, so it is not possible in any one paper to offer a comprehensive summary of what has been written. What follows is considered representative, highlighting the most salient points that would lead to opportunities for study, experiment, and development.

Though the breadth of literature available worldwide on the topic of RFID has grown explosively over the last few decades, it is not of consistent quality or credibility (Roberti, 2009). It has unsettled an establishment, as new technologies generally do. It has introduced possibilities that are not sharply limited. It relies upon physical principles that many consumers do not understand (Brookes, 2010). For these reasons, it is unsurprising that a portion of the material written overstates the abilities of RFID. A portion misunderstands the advantages. A portion misunderstands the risks. A portion is purely speculative, and lacks the testable basis to make empirical work meaningful (Hardgrave & Miller, 2006).

Literature for this review was collected by the following methods:

2.1.1 General electronic journal search

This found results from the journals indexed in the collective network of libraries cooperating with Purdue University (currently 7,634 journals). Searches were conducted of title, abstract, body, and bibliography by text strings as explained below, or by unique identifiers when a specific title had been recommended.

2.1.2 Targeted electronic journal search

This found results from top industry associations. Most prominent were the Association for Computing Machinery and the Institute of Electrical and Electronics Engineers.

A total of 23 journals from the ACM were consulted, including the SIGAPP Applied Computing Review, Data and Information Quality, Transactions on Computer-Human Interaction and proceedings of the Conference on Computer and Communications Security, International Workshop on Wireless Sensor Networks & Applications, and Workshop on Role Based Access Control.

A total of 26 journals from the IEEE were consulted, including Wireless Communications, Security & Privacy, Embedded Systems Letters, and transactions on Antennas and Propagation, Electromagnetic Compatibility, Human Factors in Electronics, and Information Theory.

2.1.3 Electronic dissertation search

This covered material in graduate dissertation work that mentioned radio-frequency identification or related electronics. Less material suitable for citation was found in this

category, but it was useful in illustrating which methods were being attempted experimentally, and what sort of success they claimed.

2.1.4 Professional newsletter recommendations

This suggested books, articles, and proceedings that others working in RFID research found useful. Much of the search for literature relied upon references in well-known publications pointing the way to subtler ones. Many valuable insights came from work that has not yet been commercialized or shared beyond academic environments.

2.1.5 Patent database search

This revealed technologies that have already been submitted for government registration in the US. Innovators that are serious enough about their ideas to seek exclusive privileges in them deserve attention here. The proposed research is not appropriate if it has already been performed in the course of a patent application.

The principle text strings used in searching by term in journals were

- "RFID privacy"
- "identification card"
- "RFID" and "driver's license"
- "RFID" and "operator license"
- "RFID" and "selective" and "disclosure" and "field" and "data"

Material published earlier than the year 2000 was considered too old for inclusion. While some valuable ideas did appear in it, they became popular enough to be published also in later material, which was cited. Sources as recent as 2015 were included in the literature search.

A subset of the results collected was selected according to the reputation of the authors and institutions with which their citations were associated. Where multiple sources described similar principles, a single source was selected as representative of the others. Material deemed redundant in established claims was excluded from the citations for the sake of bringing the list down to a manageable number. Thousands of results were initially returned, but only favored hundreds could be selected for detailed reading. Works cited by respected researchers were also explored for inclusion here.

Because broad commercial use of RFID has not been a topic of publication for more than a few decades, a publication on the topic is not considered outdated unless there is found a newer publication with content that clearly supersedes and replaces it.

Effects demonstrated publicly and made open to scrutiny were considered credible, regardless of where accounts of the demonstration might be published.

Preference was shown to established academic journals. For comments on the industry and its state, citations were limited to career professionals with terminal degrees and a background in research (and documented evidence of both available for verification). For facts on the state of the art, both these and amateur sources were cited, provided that the facts had been independently confirmed. For insight into popular sentiment and market trends, many lay sources proved useful, but they are, in the review to follow, carefully distinguished from statements of fact.

Government agencies and their publications were considered authoritative sources of government policy. Discrepancies often arise between policy and practice, but that is a matter for discussion elsewhere. Standards bodies and task forces are considered authoritative sources of their standards documentation.

Articles from disreputable sources were avoided. This includes material deemed to be composed for religious or political purposes; material lacking citations, scientific

qualifications, or scrutiny; material closely associated with claims that have already been demonstrated false; and material written in such unprofessional language as to call its content into question. All sources exhibiting one of these problems were considered disreputable until a stronger case could be found for their inclusion, where possible.

Articles were not considered if they were not published in a source accessible to Purdue libraries without additional fees, licensing burdens, or other barriers to study.

2.2 Body of Literature

2.2.1 Fundamental Concepts

The technology underpinning the RFID devices scrutinized in this study was well summarized in earlier publications from Intel Research (Want, 2004):

> RFID is an electronic tagging technology (see figure 1) that allows an object, place, or person to be automatically identified at a distance without a direct line-of-sight, using an electromagnetic challenge/response exchange. (p. 42)

Figure 1 Popular RFID Tags in Various Shapes and Sizes (Want, 2004)

An RFID system is composed of readers and tags. Readers generate signals that are dual purpose: they provide power for a tag, and they create an interrogation signal. A tag captures the energy it receives from a reader to supply its own power and then executes commands sent by the reader. (p. 42)

An RFID tag is built from three components:

- Antenna
- Silicon chip
- Substrate or encapsulation material

These tags are generally referred to as passive because they require no batteries or maintenance. Tag operation varies according to the frequency at which the tag operates. Historically, four common ISM (industrial, scientific, medical) frequency bands have been used: 128 kilohertz, 13.56 megahertz, 915 megahertz, and 2.45 gigahertz (see figure 2).

Figure 2 Two Dominant RFID Tag Designs, with their Bands and Standards (Want, 2004)

Passive tags that operate at frequencies up to 100 MHz are usually powered by magnetic induction, the same principle that drives the operation of household transformers. An alternating current in the reader coil induces a current in the tag's antenna coil, allowing charge to be stored in a capacitor, which then can be used to power the tag electronics. Information in the tag is sent back to the reader by loading the tag's coil in a changing pattern over time, which affects the current being drawn by the reader coil--a process called load modulation. To recover the identity of the tag, the reader simply decodes the change in current as a varying potential developed across a series resistance. (p. 43)

Unlike a transformer, the coils of a reader and a tag are separated in space, and coupling between the coils can occur only where the magnetic field lines of the reader coil intersect with the tag coil, the near field region (see figure 3). Beyond this distance the energy breaks away from the antenna as propagating waves that we call a radio signal; this is known as the far field region. (p. 43)

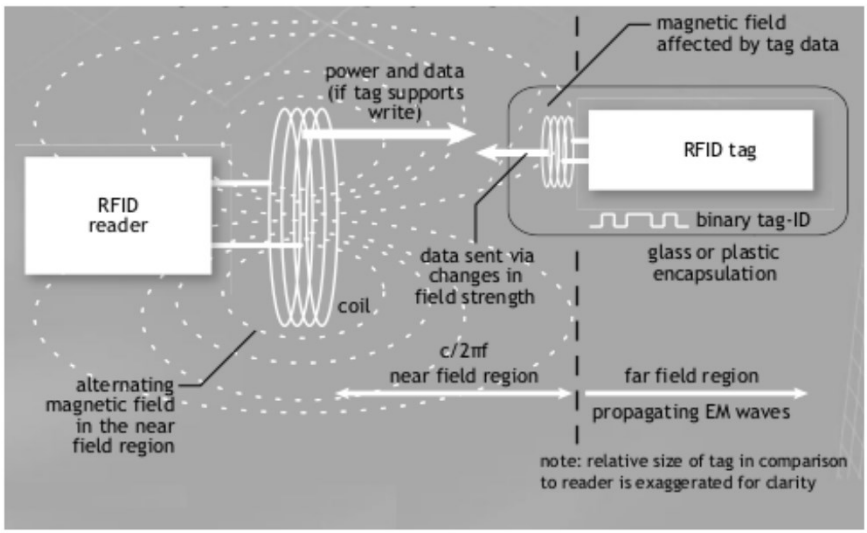

Figure 3 Near Field Wireless Coupling, as used in High Frequency Tags (Want, 2004)

2.2.2 Clarifying the Problem

The core RFID technology described above provides the means to tag entities and wirelessly obtain tag data. In short, it is a way to tell entities apart from a distance. No intrinsic mechanism for security or privacy is included in the specifications (Nogueira & Greis, 2009). Until something related arrives through additional regulatory measures, the card remains a completely passive device that will release its data whenever interrogated. In the state of Washington, for example, no security is built into RFID-enabled driver's license cards (ACLU, 2007). Users are encouraged to store the card in an enclosure and limit its exposure to unauthorized parties (2007).

Encryption has been widely touted as a means to prevent disclosure of RFID data (Mahmood & Al-Hamdani, 2011), but has not been entirely successful. The popular NXP Mifare Classic RFID chip stands as a potent example. Its encryption scheme was compromised in 2008, allowing data to be read without authorization, charges to be repeated, and cards to be duplicated for false identities (Hammerschmidt, 2008). The chip incorporated the high frequency standard mentioned above. It is used widely for personal identification, making the vulnerability especially troubling. As other encryption schemes are suggested to be stronger replacements for this one, some researchers have turned to hardware-based schemes, acting at a lower level to prevent disclosure (Lim & Li, 2008).

In a prominent RFID lab at the University of Washington, a professor of computer science and engineering lead a team of researchers in exploring at depth the social impact of this technology. In an interview about the facility (Heim, 2008) he warned that the RFID passports and driver's license cards have been designed to expose more information than necessary:

> There's no reason to have remotely readable technology in a driver's license... people don't understand the implications of information they're giving out. They can be linked together to paint a picture, one you didn't think you were painting...

> you can see this inching forward until we're tracking people wherever they go. (p. 3)

Since the public debut of RFID, Katherine Albrecht has said much about the potential pitfalls of careless deployment. Fortunately very little of what this ardent privacy activist anticipated ever materialized; but as personal identification advances, it may prove helpful to consider her warnings, because resolving consumer anxiety means putting them legally and technologically out of reach:

> During the past decade a shift toward embedding chips in individual consumer goods and, now, official identity documents has created a new set of privacy and security problems precisely because RFID is such a powerful tracking technology. Very little security is built into the tags themselves, and existing laws offer people scant protection from being surreptitiously tracked and profiled while living an increasingly tagged life. (2008, para. 4)

When security investigators at Charles University in Prague examined electronic Czech passports, they exclaimed it was "a bit surprising to meet an implementation that actually encourages rather than eliminates attacks" (para. 10).

Recall from the fundamentals section above that two families of standards have dominated the market of personal RFID solutions. The contactless national IDs and passports of most countries incorporate a tag that meets the industry standard ISO 14443 (closely related to the ISO 15693 noted earlier), which was developed specifically for identification and payment cards (Nogueira & Greis, 2009). Curiously, U.S. border cards use the EPCglobal Gen2 standard (closely related to the EPC noted earlier), a shorter-wavelength standard that was designed to track products in warehouses, where the goal is not security but maximum ease of readability (Albrecht, 2008). This is a point that shall return later in the discussion of standards for a prototype replacement technology.

A communication from the European Commission to the other European bodies listed recommendations for consumer RFID usage. Among these, that personal data obtained with this technology is subject to the informed consent of the affected individual (Krisch, 2007). It goes on to call for the ability to select when and where RFID data may be collected, which "no sufficient mechanisms" currently provide (Krisch, 2007, pp. 5-7). This directly beckons researchers to answer with something more effective than the Mifare cryptography and more specific than bulk RF shielding. Why not enable selective disclosure of individual data fields, as many or as few as might be suitable for any given transaction at any given time?

Without a sufficient mechanism for selecting the circumstances of wireless reading and tracking, no guarantee can be made that personal data has not been used beyond its intended context. This has occurred in a variety of places already, including schools where attendance mechanisms are employed (Brazy, 2010), liquor stores where age verification mechanisms are employed (Shaughnessy, 2010), entire states where drivers are licensed (McNamara, 2009), and too many other examples to quickly summarize. It is clear that concern exists on the part of consumers and citizens. Where information is available, it is sought and collected. It is used in any ways that collectors believe will become profitable or otherwise advantageous. Selecting against disclosure from the onset prevents this entire family of abuses.

2.2.3 A Call for Improvement

Of the warnings written on the various threats arising when RFID is used for personnel, many are inspired not by experience or deep knowledge of the topic, but by other, dubious influences that have not shown evidence (Galloway, 2010). For this reason, emphasis is given to those that are situated to speak authoritatively:

The vice president for government affairs at Gemalto, Inc., a major supplier of microchipped cards, is by no means an RFID opponent. He is a board member of the

Smart Card Alliance, an RFID industry group, and is serving on the Department of Homeland Security's Data Privacy and Integrity Advisory Committee. Still, he has sharply criticized the RFIDs in U.S. driver's license and passport cards. In an article for *Privacy Advisor*, a newsletter for privacy professionals, he called the cards vulnerable "to attacks from hackers, identity thieves and possibly even terrorists" (Lewan, 2009, para. 19).

Similar concerns arose from the AeA--the lobbying association for technology firms, the Smart Card Alliance, the Institute of Electrical and Electronics Engineers, the Business Travel Coalition, and the Association of Corporate Travel Executives. The Department of Homeland Security has been promoting broad use of RFID, even though its own advisory committee on data integrity and privacy warned that radio-tagged IDs have the potential to allow "widespread surveillance of individuals" without their knowledge or consent (Lewan, 2009, para. 22).

In the wake of the Sept. 11 attacks--and the finding that some of the terrorists entered the United States using false passports--the State Department proposed mandating that Americans and foreign visitors carry "enhanced" passport booklets, with microchips embedded in the covers. The chips, it announced, would store the holder's information from the data page, a biometric version of the bearer's photo, and receive special coding to prevent data from being altered (Lewan, 2009).

As gratifying as the measure might have felt at the time, it produced little in terms of measurable security for the nation, yet the price to be paid in loss of public confidence in the underlying mechanism was profound. In February 2005, when the State Department asked for public comment, this was the response: of the 2,335 comments received, 98.5% were negative, with 86% expressing security or privacy concerns, the department reported in an October 2005 notice in the Federal Register (Lewan, 2009, para. 44).

In February 2006, an electronic Dutch passport (which did incorporate encryption) was compromised on national television, with researchers gaining access to the document's digital photograph, fingerprint and personal data. Then British e-passports were hacked using a $500 reader and software written in less than 48 hours (Lewan, 2009).

In May 2006, at the University of Tel Aviv, researchers improvised a skimming device from a mere $110 worth of parts from hobbyists kits and directly read an encrypted tag from several feet away. At the University of Cambridge, a student showed that a transmission between an e-passport and a legitimate reader could be intercepted from 160 feet (Lewan, 2009).

When Michigan was pressured by the Department of Homeland Security to add RFID to driver's license cards, a state representative called upon their governor to resist, saying, "I don't think we need RFID in our licenses period, but even if we did, there is absolutely no reason it couldn't be short range and encrypted" (McNamara, 2009, para. 3).

2.2.4 Inviting the Card Overlay Solution

While much has been written about RFID in industrial engineering collections, probably the largest portion deals only with supply chain issues, such as product transportation and inventory, or with transaction issues such as cards for near-field payment rather than mag-swipe payment. When the readings are limited to those about cards for identifying people, they present a surprising few proposed solutions to the problem of unauthorized data disclosure. Many industry professionals have limited their recommendations on this topic to the usual prudent advice: keep the card in an RF shield when it is not in use, and expose it only in range of desired scanning. Since active tags typically are not used for personnel cards, that range is on the order of meters rather than kilometers.

There have been hardware designs intended to make undesired scanning more difficult, such as adding switches that only enable reading while the card is being pinched in the user's fingers (Huber, 2012), but they still dealt with complete disclosure of the data. No design was found in these sources that provides a hardware mechanism for disclosing only particular fields of data. That is what prompted its investigation here.

Many of the functions performed with RFID are also possible with alternative technologies, such as digital image processing (Gregorio, 2009). For the sake of focus, the principles of effective identification shall be applied here only to RFID technology, and in light of the violations to RFID cryptography mentioned earlier, this investigation narrowed further to include only hardware-based mechanisms.

There have been software mechanisms for this purpose (Rieback, Gaydadjiev, Crispo, Hofman, & Tanenbaum, 2006), but these obviously operate at a higher level of abstraction, and rely upon obstructing the flow of data through code, rather than preventing the electrical signals from ever leaving the card. Building security into the device closer to the hardware can help to prevent these problems, serving as an effective replacement or companion to cryptography. This is a distinction that shall be explored further below.

A trend has been rising in street-corner shops that are under legal requirement to verify the age of their patrons. There are documented stores that not only check, but also record ID card information when they make alcohol sales. Devices such as the Z22 CounterTop ID Checker are capable of automatically scanning driver's license cards, retaining thousands of their records in onboard memory, or transferring them to external computer networks (Shaughnessy, 2010). This encroachment means that the consumer is further limited in his ability to control personal data, and prevent future abuses of it. Data fields that are not involved in the age verification process are relinquished whenever the age field is examined. The data, once collected, leaves the owner's control and may be stored or processed in whatever manner the collector deems appropriate.

One of the earliest and most valued contributors to RFID security was Simson Garfinkel who, with the aid of two colleagues, published several ideas that seem especially noteworthy as having directly influenced the research proposed here. The first is what became known as his RFID Bill of Rights, a set of five guiding principles for system creation and deployment similar to those established over many decades of identification using other technologies.

The Bill states that users of this technology have:

1. The right to know if a product contains an RFID tag.
2. The right to have embedded RFID tags removed, deactivated, or destroyed when a product is purchased.
3. The right to first-class RFID alternatives. Consumers should not lose other rights (such as the right to return a product or travel on a particular road) if they decide to opt-out of RFID or exercise an RFID tag's kill feature.
4. The right to know what information is stored inside their RFID tags. If this information is incorrect, there must be a means to correct or amend it.
5. The right to know when, where, and why an RFID tag is being read. (Garfinkel, Juels, & Pappu, 2005, p. 41)

Note that this list deals with policy matters, rather than the mechanisms of assurance. It is a reminder that sound regulatory principles are vital to RFID success (though beyond the scope of this dissertation). Nonetheless, they cannot be put into effect without some underlying mechanism, so it would seem to invite the work proposed. The fifth point is probably the one best served by a model of selective disclosure, and it is a point highlighted here as vital.

The team recognized a way that selection could occur:

> The farther away a reader is, the greater the noise level in the signal a tag receives. With some additional circuitry, therefore, an RFID tag might be able to obtain a

> rough estimate of the querying reader's distance and change its behavior accordingly. A tag interacting with a distant reader might only reveal the type of product it's attached to--a pair of trousers, for example. When interacting with a nearby reader, however, the tag might also reveal its unique identifier. A more sophisticated, multi-tiered approach is also possible, in which tags furnish increasing amounts of information as readers get closer. (p. 41)

Though this approach might be of interest to inventors, distance clearly is not always the most suitable selection factor in common consumer or citizen cases. Regardless, it is important to recognize that containing the intelligence begins with low-level antenna signal viability, which is precisely what the approach illustrates. If the card cannot be sufficiently charged by the wireless reader (a process known as excitation), it cannot produce the signal to reply. The card operates in "half duplex", receiving energy first and only afterward transmitting any. The reader then accepts the returned signal data, and singulates the tag accordingly.

These researchers also draw attention to the concept of blocker tags, fully described by Juels, Rivest, & Szydlo:

> The RFID blocker tag takes a different approach to enhancing RFID privacy. It involves no modification to consumer tags. Rather, the blocker tag creates an RF environment that is hostile to RFID readers. The blocker tag is a specially configured, ancillary RFID tag that prevents unauthorized scanning of consumer items. In a nutshell, the blocker tag "spams" misbehaving readers so they can't locate the protected tags' identifiers. At the same time, it permits authorized scanners to proceed normally. (Garfinkel et al., 2005, p. 40)

As a mechanism of rejecting unauthorized readers, this is an intriguing solution. What is developed below, though, is a mechanism that provides the means to select and authorize fields on the card itself. As the authors correctly noted, the privacy concern of

RFID devices arises between the user, the card, and the reader. It is possible to create a solution in one that causes no new interference to another.

The solution put forth here is expressed in terms of the following principles:

2.2.4.1 Custody

In existing personal ID applications, if a card is scanned, its entire contents are obtained. If only a portion of that information is needed for the action at hand, the scanning party is expected to exercise discretion by deleting the remainder. On occasion, it is not deleted, but finds its way into other actions, including unauthorized actions. There are three major ways this can occur in the existing approach:

- Sincere Accident (as an embarrassing disclosure of one's age, weight, etc.)
- Function Creep (as the liquor stores' growing customer databases, etc.)
- Malicious Misuse (as a malefactor who commits fraud with ID, etc.)

If the technology within the card does not release private information, then there is no need to look after it using technology outside the card. The card (and thus its holder) retains custody of the information. There is no need to confirm that such information has been securely deleted, seeing that it was never available for abuse. Wherever possible within the regulatory framework, this approach is appealing for its simplicity and apparent effectiveness.

2.2.4.2 Mechanism

What this work contributes to the RFID industry is a model that does not rely upon the competence, morality, or technology of the party performing the scanning, but instead builds into the card itself the means of selective disclosure. This principle of placing impersonal mechanisms above personal promises removes the opportunity for entire families of misuse and crime. It enables the user of the card to be more directly responsible for the disclosure of information, and any consequences that might follow.

2.2.4.3 Prevention

Much of the work done to address privacy compromised through RFID has dealt with response measures. Indeed, controlling loss is often best done by early reporting, repudiation, and re-issuance, etc. Where users receive guidance on preventative measures, it's frequently about looking after the card and the information it contains. A user's ability to do this is greatly reduced by several factors in the RFID card design:

- Information may be read from the card without the holder's knowledge.
- Reading of the card is possible even if the holder refuses.
- The holder has no means to choose which data fields are read.

The design presented here replaces the information pathways that had been permanently open with gateways that may be closed, preventing misuse of the information, so that the reactions never even need to be addressed. One of the great conveniences of RFID is that it can operate through an opaque container such as a wallet, without needing to be removed. This can become one of its great problems if there is not also available a simple way to contain the data when an operation was not intended.

2.2.4.4 Empowerment

Just as it is unrealistic to advise preventing an action that has no feasible barriers, it is unrealistic to advise RFID users to take prudent measures if such measures are not within the holder's legal or physical reach. By adding a mechanism for access switching to the card that the holder may easily set in a readable or unreadable position, the design change empowers him to make the decisions and assume personal responsibility for them. This brings not only greater assurance to the holder, but also reduced liability to the issuer and reader. Much of RFID security has been invisible, even when it is working well. Best practices in identification, and many other systems, call for active and visible reporting. "It's not enough to make someone secure, that person needs to also realize they've been made secure" (Schneier, 2008, para. 12-13).

2.2.4.5 Least Privilege

A fundamental principle of information assurance is that any given party should be granted access to only as much information as necessary to complete the desired objective (Amer & Hamilton, 2008). Frequently, though, an article of identification such as a driver's license is used to establish a link between only two fields such as a photograph and a name or a photograph and an age, etc. even though many other fields are included on the card. For printed cards, this matter may be overcome easily enough by obscuring those fields (with tape or the like), and making them temporarily unreadable. For radio-frequency cards, though, there is no intrinsic means to suppress one field while leaving another available. It is for that reason that this design is being introduced, so that information fields may be shared wirelessly, on a need-to-know basis, with no additional fields packaged along with them.

2.2.5 Design Factors

The RFID card design described in this paper is intended for widespread adoption, as a state or national identification document. As such, its logistics deserve some explanation. Attractive alternatives to cards are available in the form of various smart devices, etc. (Metras, 2005). Why then might the cards be preferable? Here are some of the most significant factors that, in the context of this dissertation, border and direct the path to the intended ID solution:

2.2.5.1 Cost

To fulfill its purpose, the device must be affordable enough to be available to an entire population. If the cost of a smart phone on which to run an identification application is beyond the means of a user, then routine ID tasks will become unavailable with it. Likewise, if the cost to produce and maintain the device are much greater than the current cost of government ID documents, the responsible agencies will be under burdensome economic pressure. In the United States, even a slight increase in costs will be multiplied by a population of over 3 million people (US Census Bureau, 2013). The solution must be exceedingly affordable, in terms of not only the materials, but also the manufacturing process, distribution methods, and total operation after deployment.

2.2.5.2 Durability

ID documents that are issued for use over a period of five or ten years will clearly need to be made of materials that can withstand harsh handling. They may be carried daily in pockets, wallets, purses, or lanyards. They will be flexed often, and subject to temperature extremes. They will get wet. They will be dropped. They will be exposed to electromagnetic interference. To remain useful, the device must be resilient. This makes even card technologies such as electronic ink or touch-sensitive surfaces seem impractical. The electronics of RFID are, themselves, vulnerable to some sources (Juels et al., 2003), but they represent a mature technology that is in widespread use today. Card durability is well established in consumer environments, even under many harsh conditions (Xiang-jie & Hua, 2014).

2.2.5.3 Size

The maximum dimensions of a device in regular use would probably be the passport, which itself is too big to fit in a common wallet. An ID device much larger than a driver's license presents a nuisance to the user that had previously stored a pocket-sized card. A design that had switches or connectors extending out from its surface would cause it to catch often on its container and on garments, and risk damage to both. It seems preferable, then, to use a smooth card with a form factor no larger than about 9cm by 6cm on its face, with a thickness no greater than about 1mm that does not require any outer covering thicker than 300μm.

2.2.5.4 Simplicity

It seems favorable to offer users a solution that exhibits security they can understand and privacy they can control (Smith & Spafford, 2004). Neither is possible in a system of profound complexity. A solution that operates at a lower level of abstraction is preferable to one at a higher level. One that is hardware-based, and thus able to function even below the software that might be run above it, is preferable to one that depends upon its software platform and its changing maintenance schedule. As discussed earlier, simplified RFID mechanisms for feedback and control have been demonstrated. Here they are applied in a manner that offers the user a simpler explanation.

2.2.5.5 Familiarity

The user is a major cause of ID device failure, often caused by misunderstanding complicated technologies (Marqhardt et al., 2010). It is helpful, then, to deploy a product that has the look and feel of the cards already in use. The steps taken in using it should parallel steps taken with the earlier (print) cards. Where it is possible, it is beneficial to make the operation of the device intuitive and transparent. Where it is not, the designer might at least make the device behave in ways that suggest what is happening internally, so that users will be more likely to act accordingly. When technology serves human needs well, it often becomes so subtle it is taken for granted.

2.3 Converging on the Topic

It is clear from the literature that where RFID and information assurance intersect, a great variety of research opportunities arise. As discussed above, they narrow down from the general and numerous topics to the one specific topic addressed in this dissertation:

At the broadest level is the specter of identity "theft" and misrepresentation. This would include all conceivable ID documents and means of misusing them. It would also include the various ways to prevent misuse, and among these is the topic of access control for documents. As far as the type of document is concerned, all the most popular were studied. The passport was considered, of course, and the Social Security card, but special emphasis fell upon the state driver's license cards because of how widely they are carried and how often they are requested as a form of identification. The history of misuses involving a driver's license is still too large to deal with, particularly in light of current changes to the cards, so the factor of radio-frequency identification was considered particularly. A transition is occurring between printed cards and electronic cards, so it would seem a good time to bear down upon RFID for a card akin to the driver's license, or certainly something using its same pervasive form factor. It would need to be something small enough to fit in a wallet and be carried in the same way as the license. It would need to be affordable enough and durable enough that states and nations could scale deployment plans to include entire populations. Within all these constraints, an opportunity is found to further narrow the work to the prospect of documenting a mechanism for card data selection. It reworks established methods of intentionally detuning the antennas of an RFID card, using the particular overlay solution described in the Methods.

2.4 Prior Works

To help ensure that the design and function of this solution are in fact unique, an exhaustive search was made in the database of the United States Patent and Trademark Office. The text and illustrations were read for every patent since 1976 for search criteria germane to RFID card technology. All of the results returned were reviewed. Complete details may be found in the Appendix section.

None of the patents read incorporate a multiple-region card of this type, nor the selective detuning method described in this dissertation. Those patents that do incorporate aspects of the same work are distinguished accordingly. While it remains a matter for patent agents to argue, the proposed design appears novel, and deserving of a rigorous investigation.

CHAPTER 3. METHODS

3.1 Design Objectives

The introduction and validation of a novel RFID overlay solution was a necessary part of this research. Existing RFID cards used to identify personnel suffered from the limitations mentioned above, but an alternative card that was shown to overcome these limitations has been produced, inviting a discussion of the technologies used in it, and the prospect of deploying it for large-scale public use. Its first purpose was to be used here in response to the stated Research Questions:

a) Is selective detuning a feasible mechanism for independent selection of RFID card data?
b) Can a design for selective RFID detuning operate reliably enough to be practical?

Shown in figure 4 is the outward design of a popular RFID personnel card. Other than labels for the manufacturer's registered trademarks and an arbitrary decoration, the surface is blank. It conveys no visual descriptions of the data it contains or is prepared to release. There are no input devices on the card, and no indication of which regions on the card are most susceptible to detuning. Of particular note, there is no separation of its data fields (or references to fields); the card acts as a single monolithic container. When it is read, it releases all the fields (or a unique identifier that may be used to obtain all the fields). Until some external device has received and acted upon it, the output set is indivisible.

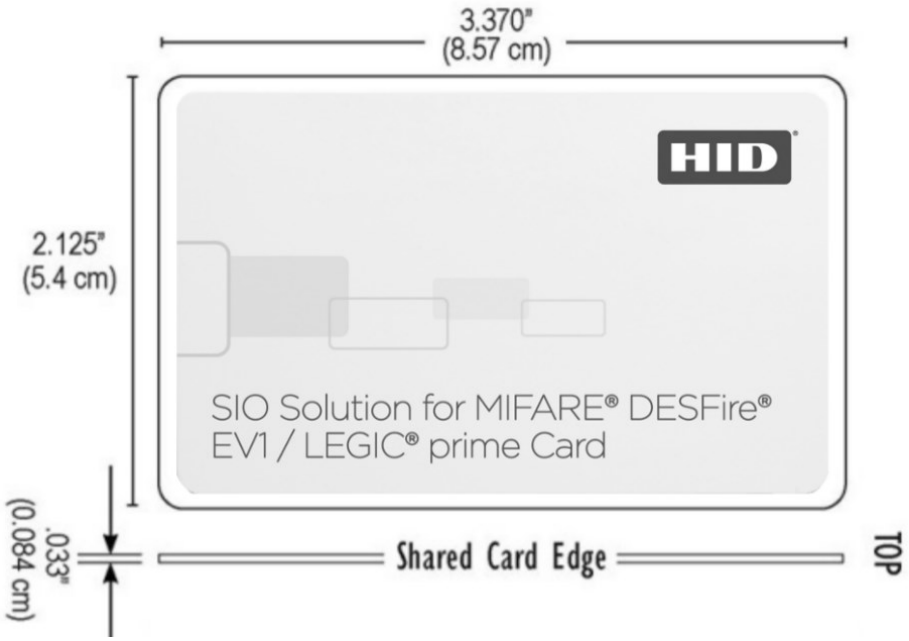

Figure 4 Commercial RFID Card (HID, 2014)

The antenna inlay used inside this type of card is shown in figure 5 (2014). Its flexible coil follows the perimeter of the card in a nearly symmetric pattern.

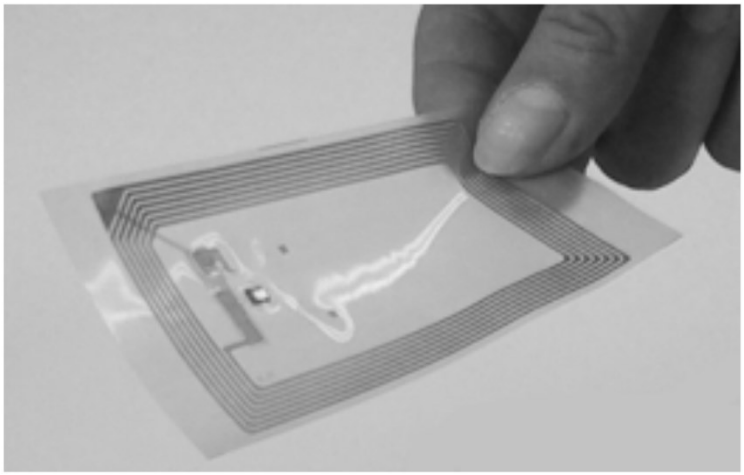

Figure 5 Antenna Coil Pattern of Common RFID Cards (Cram, 2014)

In contrast, the demonstrated model uses separate antennas, each of which forms an oblong coil. They are located in RF-sensitive regions that correspond to regions on a

printed card, but are insulated from it and are visibly labeled accordingly (see figure 6). Access to the data represented by each region may be toggled by obscuring that portion of the card with a conductive tape. This analogy makes the device behave in a familiar, intuitive way to the user, and does for RF visibility what it does for optical visibility. What the experiments were designed to test is whether an overlay of common aluminum tape would offer reliable coverage when used with the prototype card, changing it predictably from the readable to the unreadable state according to the exposure of the region.

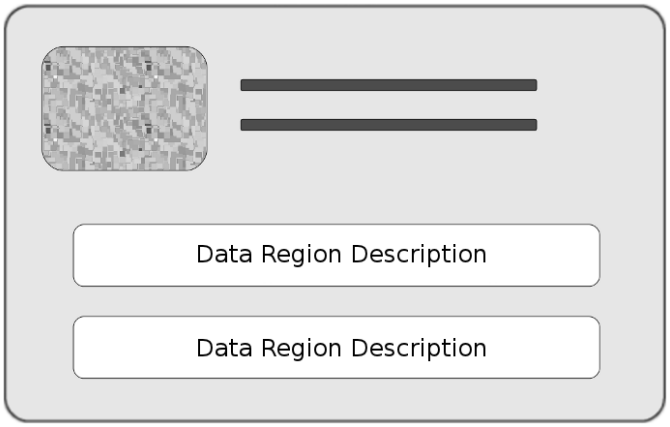

Figure 6 Labeled Prototype Card Surface

In studies concerning disclosure from printed cards, other researchers have done work with preformed opaque sleeves (Clement et al., 2012). These serve the same purpose as the tape, but allow for faster changing and easier storage. The findings of this study on pieces of tape coverage would transfer well to preformed sleeves of aluminum, and likely of any similarly conductive material. The aluminum tape was used here for three reasons that concern the end user: it is reasonably affordable, it is readily available, and it is highly variable. Less precise than machine-cut overlays, tape varies greatly as it is cut or torn by the user. Showing that it operates reliably even with a broad tolerance for the geometry of the overlay would allow a developer of this card to confidently claim that the machined overlays would perform at least as well as the tape overlays.

The aluminum portion of the overlay was electrically continuous, and had no gaps within each data field. The total thickness of the metallic layer and its attached adhesive layer did not exceed 100μm.

A successful read outcome was one in which the obscured data fields of the card were concealed, but the exposed data fields were revealed. All other possible outcomes were considered error conditions, and counted accordingly. The number of errors amassed was analyzed statistically. Both the state of the field in question and the read outcome were considered categorical variables, and both were assigned binary values. Any read condition that failed to read the entire contents of a data field during interrogation was considered a negative outcome. All others were considered positive.

3.2 Experiment Design

From each of the two Research Questions first posed in the Introduction follows a testing track suitable for its inquiry. The hypotheses, variables, and experiments are separate for each of these tracks, and the statistical tools applied accordingly. Data were collected for each, and their patterns lead to two sets of results. From these, the unified Conclusions section was composed.

3.2.1 Test 1: Independence

[from Research Question A]:
Is selective detuning a feasible mechanism for independent selection of RFID card data?

It is necessary to test whether there exists a relationship between the overlay coverage on a given data region of the card and the readability of other data regions. What is needed from a usable design is that no region of the card be detuned by overlay coverage outside its region.

3.2.1.1 Hypotheses

3.2.1.1.1 H0a

Access to the data of a given field will not depend upon the overlay coverage of a field other than its own.

The hypothesis stands unless access exhibits dependence on coverage of a region of the card other than the region labeled for its own field. That is, the test fails to reject H0a if the state of coverage for one region of the card does not reliably correlate with readability of data from the other region.

3.2.1.1.2 H1

Access to the data of a given field will depend upon the overlay coverage of a field other than its own.

The hypothesis stands if access exhibits dependence on coverage of a region of the card other than the region labeled for its own field. That is, the test rejects H0a if the state of coverage for one region of the card reliably correlates with readability of data from the other region.

The value of α chosen in this test was .01, for a confidence level of 99%.

3.2.1.2 Variables

Involved in the direct effect testing:

X Independent - coverage state of region (binary categorical)

Y Dependent - readability of region (binary categorical)

Recorded for procedural purposes in the laboratory:
region under test (binary categorical)
current pass (scalar) and pass count (scalar)
current orientation (trinary categorical)
readability_roll
readability_pitch
readability_yaw

3.2.1.3 Data Collection

Before testing the effect of the card's overlay mechanism, it was necessary to test the laboratory equipment and the core RFID technology. A baseline test was conducted, in each of the 3 axial orientations, with the card's data regions completely exposed. All the equipment passed. With the baseline complete, samples were taken with the data regions completely obscured. Results were compared to the baseline. Then, to make certain that the suppression of the obscured fields had been temporary, and had not resulted in any lasting effect to the card, additional samples were taken completely exposed. The equipment performed without malfunction, according to its normal advertised operation.

One of the two data fields was randomly selected for treatment in the first testing course. It was completely obscured, while the remaining field was completely exposed. Samples were taken in each of the 3 axial orientations. The second testing course proceeded in similar fashion with the coverage states exchanged, for an equal number of samples. Data were aggregated and compared against cycle count to obtain the total fault count. It is considered a "transfer fault" if the reader fails to obtain data from an exposed region of the card, and a "blocking fault" if the reader obtains data from an obscured region.

The purpose of dividing the total run into 3 subsets is to represent the 3 axis of rotation. This serves to control for variation that might arise from the orientation of the card as it is presented to the reader. Cards were swept through the entire range of motion during each read attempt, and the results were separated according to axis so that any effect arising from orientation might be correlated with it during the statistical analysis.

As the arrangement also controlled for the rotation of the card as it approached the reader, it was important that the sampling be allowed to run for several thousand cycles in each record set, giving good opportunity for any card anomalies to be observed and separated from the effects of the overlay. Card antennas are not isotropic radiators, but rather do exhibit nulls, similar to the nulls at the ends of a dipole radiator, that may be clearly observed at a distance. They become increasingly less observable as the distance is reduced. Allowing the cards to rotate through their entire range of motion helped to ensure that any nearby materials that might have acted as parasitic radiators affected the entire set of subjects, with minimal bias (see figure 7). The card's own driven element was the only apparent source of backscatter.

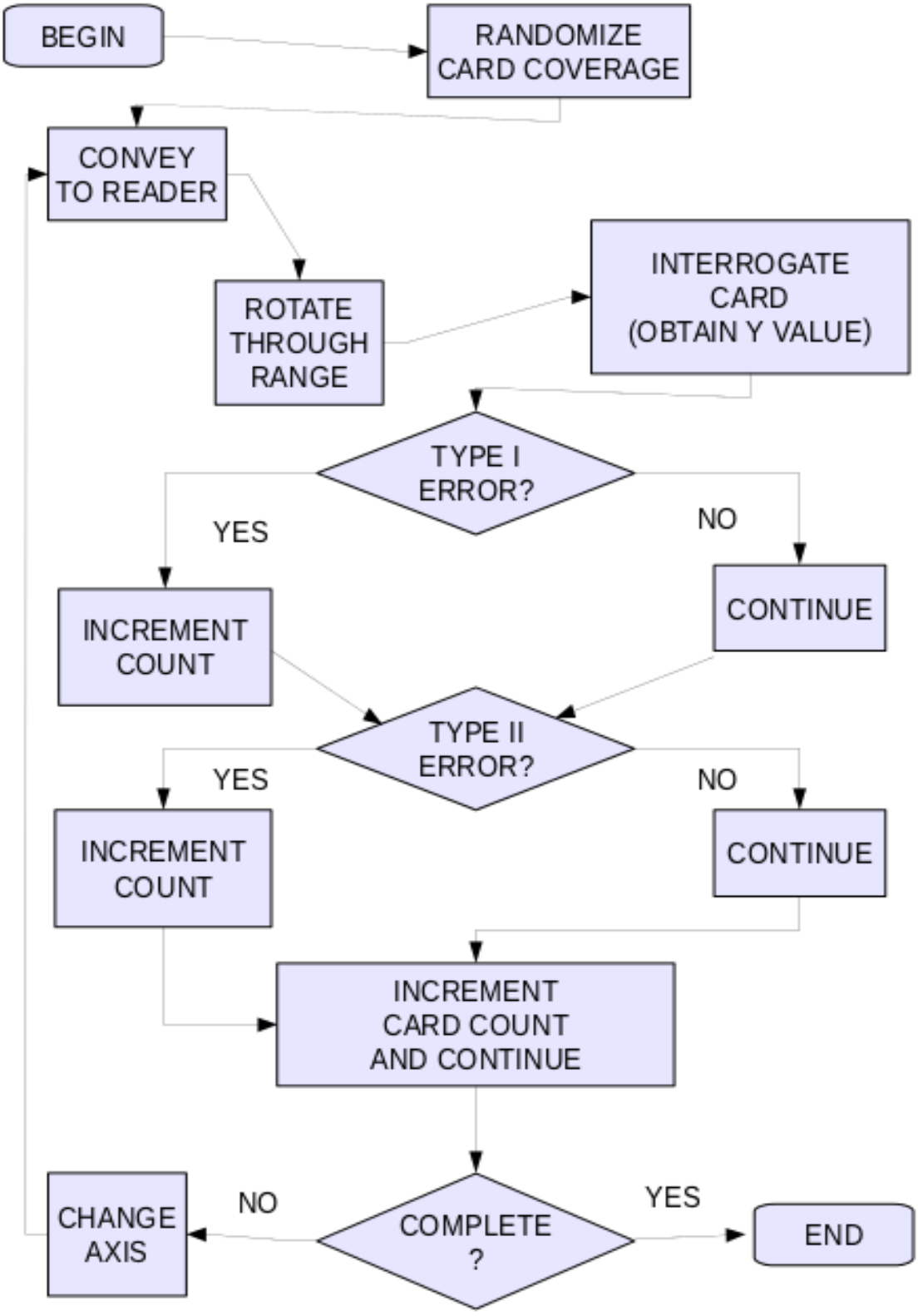

Figure 7 Test I Experiment Flow

3.2.1.4 Statistical Analysis

The statistical significance of a variable's deviation may be found by comparing it to a χ^2 distribution (Cook, et al., 2001). This is among the most straightforward ways to test the independence of two categorical variables, which is precisely what was needed in this experiment. The relationship between the concealed region and the overlay coverage of the concealed region was tested, as was the relationship between of the exposed region and the coverage of the concealed region. This was done for each region's data against the opposing region's coverage to test whether it was possible for any of the coverings to affect data outside the boundaries of their respective regions. A test was then conducted for the relationship between the concealed region and its own coverage, to confirm that the covering directly affected data within its boundaries.

3.2.2 Test 2: Reliability

[from Research Question B]:
Can a design for selective RFID detuning operate reliably enough to be practical?

For the card design to be practical in the hands of its users, it must function with an inconsistent overlay. If the aluminum tape is used, there may be variation between one application of the tape and another. The card must present a range of coverage within which a given field will assuredly be concealed and beyond which it will assuredly be readable. Just as the user name on a printed card field does not become completely readable if a mere 10% of the text is made visible, so this RFID card must not become completely readable if a mere 10% is made scannable, etc.

To test the variety of ways the aluminum overlay might be cut for use on the card, the pattern itself was randomized. The chosen region began with an overlay that completely obscured it. Each reduction was made with a single linear cut, separating 50% of the remaining material from the missing portion. The angle of the cut included the

polygon center--the point equidistant from each vertex--and followed a randomly selected line through half a unit circle, or π radians, describing the overlay (see figure 8). A new angle was chosen for each cut, and half the material was removed for each set, until its effect was deemed negligible. This occurred when read operation succeeded in spite of the overlay more often than 1% of the time in the testing course.

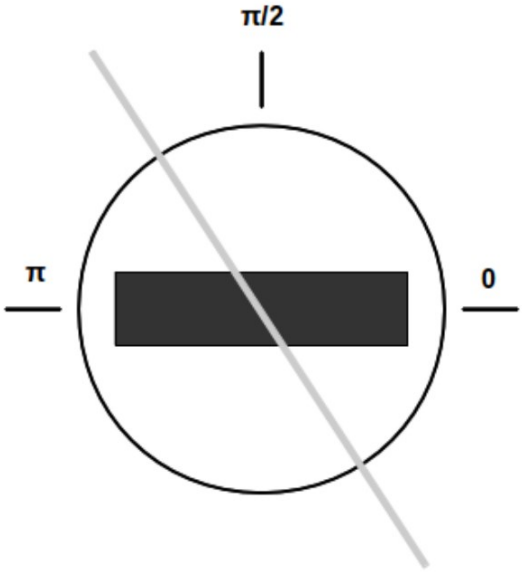

Figure 8 Reduction Guide for the Overlay

To illustrate that the tapering of the observed effect is, in fact, caused by the tapering of the true effect, one additional testing course was taken, at one additional overlay reduction, beyond the course in which the 1% threshold was met. Only when the effect was observed in more than one successive course did the reductions and testing halt.

3.2.2.1 Hypotheses

3.2.2.1.1 H0b

The effect of the overlay will not show a predictable decline as its coverage is reduced.

The hypothesis stands if the transition effect from covered to uncovered state is not sufficiently pronounced. That is, the test fails if the graph of the effect trails off gradually through the transition rather than falling abruptly. The coverage area of the card regions were decreased logarithmically as the test continued, and the reliability of the read attempt recorded. If the effect is pronounced and reliable close to the transition point, then it should exhibit a significant difference across samples with different coverage areas, but not a significant difference among samples of the same coverage area.

3.2.2.1.2 H2

The effect of the overlay will show a predictable decline as its coverage is reduced.

The selective tuning design is considered reliable if its outcomes with respect to coverage percentage are so predictable as to beat chance at the stated confidence level.

The value of α chosen in this test was .01, for a confidence level of 99%.

3.2.2.2 Variables

Involved in the direct effect testing:

X Independent - coverage percentage of region (categorical)

Y Dependent - readability of region (binary categorical)

Recorded for procedural purposes in the laboratory:

region under test (binary categorical)

current pass (scalar)

pass count (scalar)

current orientation (trinary categorical)

number of unsuccessful interrogations on an exposed region.

number of successful interrogations on the concealed region.

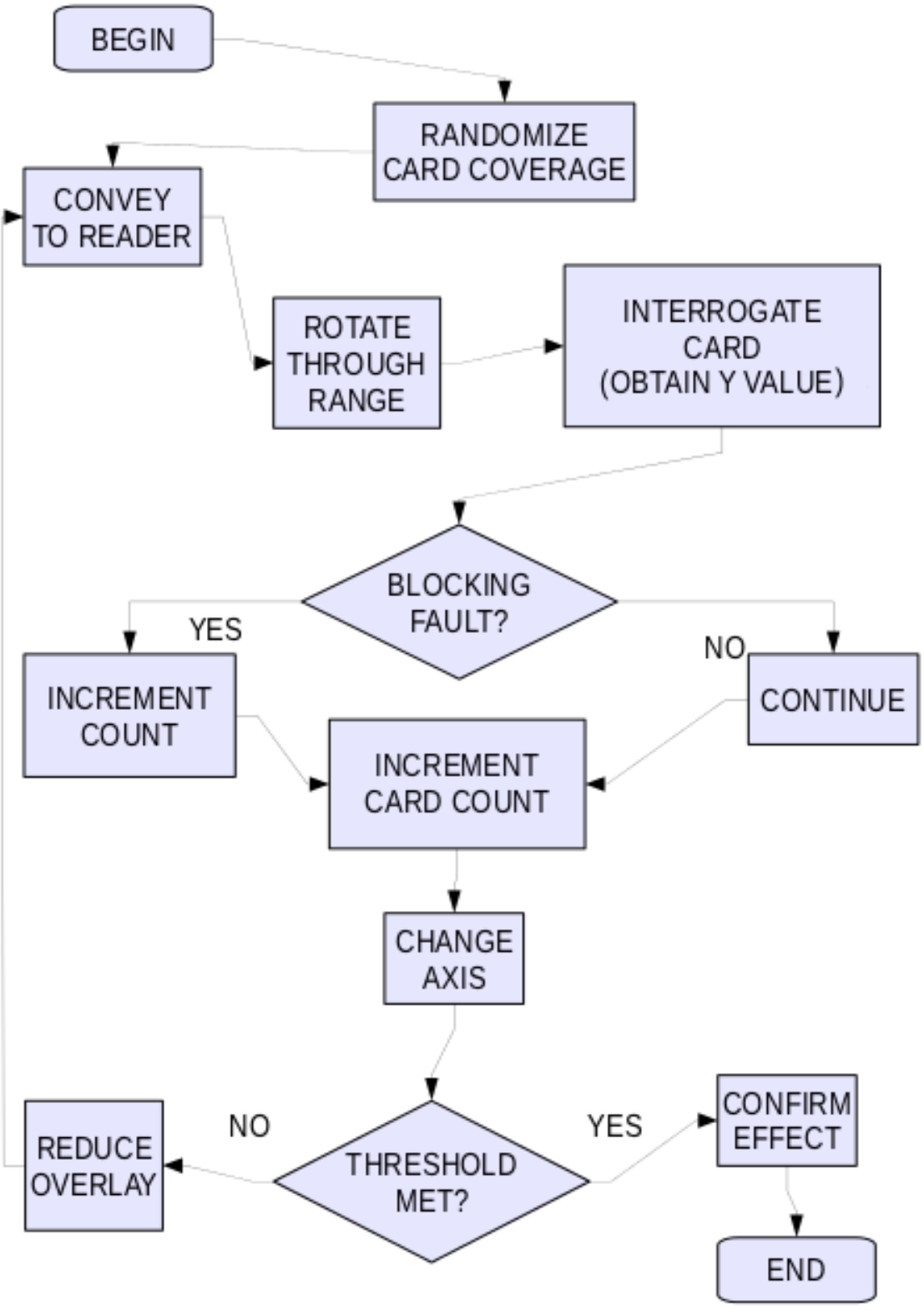

Figure 9 Test II Experiment Flow

3.2.2.3 Statistical Analysis

A binary logistic regression was plotted to test the relationship between the coverage of the target data region and the readability of the region. For the hypothesis of reliability to be accepted, there needs to be evidence that the difference between a readable and an unreadable region strongly correlated with its overlay coverage. Further, the transition region that occurs as the surface area of the overlay is reduced should be narrow, signifying that overlay dimensions exhibit little uncertainty. The binary distinction between an exposed region and a concealed region should be sharp.

3.2.3 Experimental Protocol

These are the details of the experiment that are common to the two tests above.

3.2.3.1 Subjects

Each subject unit of this experiment was a pass of the card through the RF field of the reader at a specified coverage and range of orientation. The process was automated by means of a mechanical conveyor, and require no human subject participation. While it could be argued that human bodies might impair readability of the card by adding field blockage or detuning, there is no apparent means by which they might *improve* readability of a card that has been obscured as unreadable. For this reason, card processing is automated. This served the interest of time, so that many cycles of the test procedures could be run, and statistical power strengthened.

3.2.3.2 Instruments

The experimental card design is a customized passive RFID tag system that used 13.56MHz ISM-band signaling. To verify that the overlay causes only one of the data

fields to be obscured without affecting the others, the card surface was divided into two labeling regions. Silkscreen marking on the surface corresponded to antenna boundaries in the substrate below (figure 10).

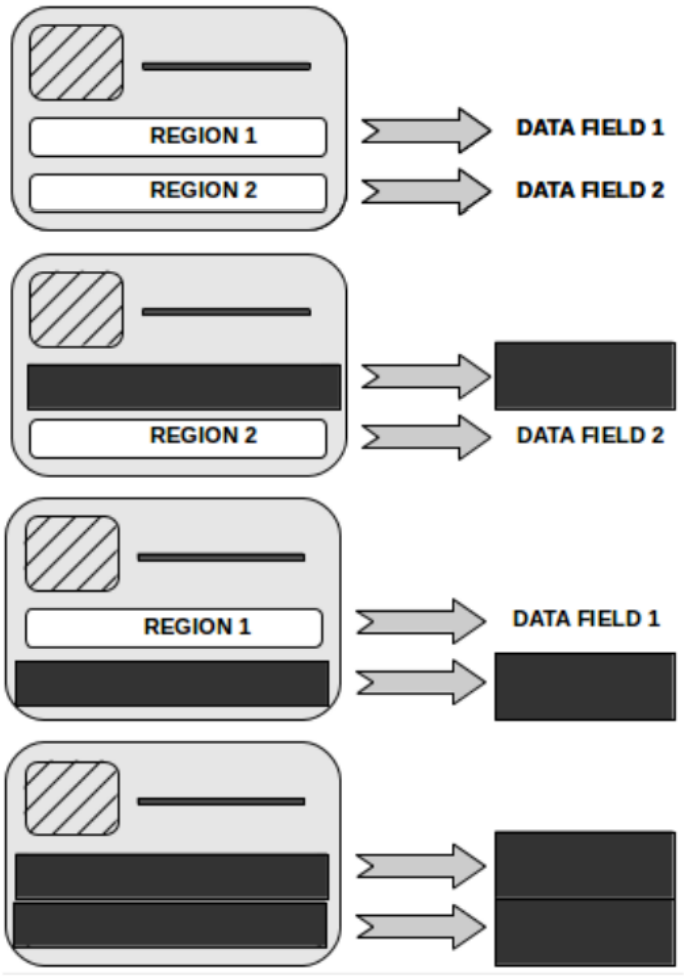

Figure 10 Obscured Fields, and the Data Released

The reader was an ordinary ISO-14443 commercial board connected to the computer system via USB port, and to a commercial antenna inside a common polypropylene radome operating in unobstructed space, with a radiation lobe focused on a point midway in the conveyor path (figure 11).

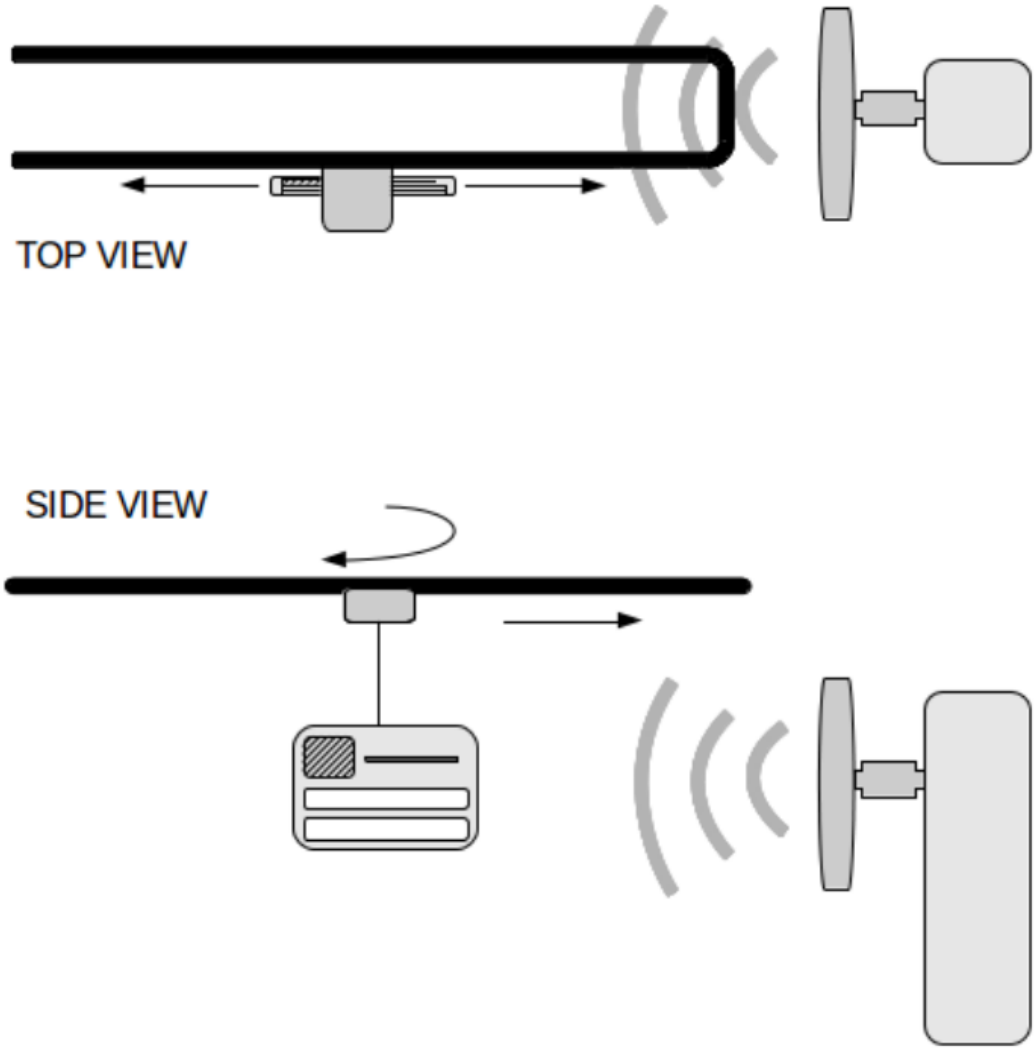

Figure 11 Card, Conveyor, and RFID Reader

Any variation attributable to the direction of approach was controlled by approaching the read antenna from both directions, as shown. The apparatus was mounted far enough to carry the card beyond the confirmed read range, and close enough to pass through the antenna's near field. The configuration was similar to the robotic positioning system used in the Georgia Tech RFID testbed. It was needed because card performance can vary according to position in space (Johnson, 2008).

3.2.4 Laboratory Conditions

The card used in the experiment was designed for symmetric wireless regions, and constructed to minimize internal interference. The active regions were selected by detuning a portion of the onboard antenna with aluminum tape. A brief trial run was conducted for both the exposed, obscured, and partially obscured states to ensure that no apparent defect or bias in operation was visible. Card coverage was selected randomly without replacement to represent either 01 or 10, where 0 indicated that the region should be exposed and 1 indicated it should receive an overlay.

It is considered a Type I error for the reader to record an unsuccessful interrogation on an uncovered region. Note that this may be confounded by factors such as

- Background radiation
- Electrical utility glitches
- Damage to the card
- Physical obstruction
- Insufficient dwell time
- Wireless signal collisions

To control for these factors, the test were conducted in a prepared laboratory environment. A Geiger counter sweep confirmed that no significant ionizing source of radiation was present during the testing, and any interference from nuclear emissions was naturally occurring, at under .04mR per hour. A broadband field strength meter was used to confirm that non-ionizing background radiation was likewise no higher than the ambient noise floor, and at least 30dB below the manufacturers' advertised threshold of interference for the reader device. The temperature of no surface or air space was outside of a range from 20°C to 30°C. Humidity was controlled to between 40% and 50%, and barometric pressure was between 990hPa and 1025hPa. Personnel were in contact with 0V-reference dissipative straps during work to prevent electrostatic discharge. Test

instruments were powered by a conditioned, uninterruptible electrical circuit at 125VAC+/-2%.

The cards used in the test were recently manufactured, inspected thoroughly on site, and handled with sufficient care as to prevent wear. The test apparatus provided an unobstructed line of sight between the interrogator antenna and the RFID card, passed it through the range of operation slowly enough to provide dwell necessary for a read operation, and avoided collisions with the radio fields of nearby cards by physically isolating the card under test.

It is considered a Type II error if the reader records a successful interrogation on a covered region. This may be confounded by factors such as

- An inconsistent bond between the cover and card
- Damage to the cover material
- Misidentification of the card under test
- Active interference

To control for these factors, the cover was fabricated from a tape of consistent manufacturing specifications, for which the aluminum and adhesive layers together did not exceed 100μm in thickness. This was applied directly to the card, with no additional buffer in between, and no cracks or wrinkles in the cover. In successive trials, the fields were swapped, which would have exposed the effect of any lasting damage to one field.

The cards used in this experiment were programmed with unique identification tokens, and as mentioned above, the test was conducted in an isolated environment, beyond the range of any card that might be misidentified as the test subject or other wireless device that might have interfered with the test to such an extent as to trigger a positive response.

The question of usable range often arises in RFID discussions. There is no decisive answer on how far away a card may be used with a reader until it is specified what type of reader, antenna, power level, etc. are used in what environment, with what radio landscape, etc. Cards of this type are often categorized as "proximity" tags, intended for use within about 1m of a reader under normal operating conditions (Nogueira & Greis, 2009). This would easily satisfy conditions where a user might hold out a card before a reader on a door, etc. The experiments outlined in this paper took this into account with a testing apparatus placing the tags no farther than half the maximum distance published by the manufacturer.

As it is vital that obscured fields on the card are rendered unreadable for as long as the overlay is in place, the card's distance from the radome was not measured as a variable. Rather, the entire usable range was involved. Each pass began at a point considered unusable for reading, swept through the closest usable proximity to the radome, and continued until again beyond range. Successful interrogation at any distance in this range was considered a successful outcome.

The card was exposed to the maximum effective radiated power available within the constraints of the reader system and FCC regulations, to rule out the possibility that the overlays are only effective at lower power, as license and passport covers are (Lewan, 2009). While this does not disprove that devices operating at unlawfully high power might yet be able to penetrate the overlay, it is sufficient for the purposes of a prototype. As mentioned earlier, the mass production design would use a switching method that is not diminished even if the radiated power is increased.

The orientation of the card remains a source of uncertainty in read success rates, so sampling was done on all three axis of rotation, using a dielectric swivel on which the card might rotate freely through its entire range of possible orientations. By connecting this to a servomotor rotating at a rate slow enough to prevent read interference yet fast enough to keep pace with the conveyor system, it was possible to expose both sides of the

card, at every angle with respect to the radome. While it would be possible, in practical settings, for the card to find itself in oblique orientations that would require spherical coordinates to describe, the radiation pattern advertised for the type of antennas used in the experiment covers these orientations as readily as those on orthogonal axis (Philips, 2002). For this reason, 3D rotation is considered rigorous for removing this variable during testing.

It was vital that the experiment demonstrate not only that the obscured data field became unreadable, but also that the exposed fields did not. It has already been established that storing the card in a suitably shielded enclosure, under normal operating conditions, will reduce the readability of every field (Koscher et al., 2009). What was needed here was the means to select desired fields to be read while leaving all other fields unaffected. For this reason, the field to be obscured in each testing was randomized, and the read outcomes were recorded for all fields during every pass through the reader.

As each testing set was satisfied, half of the remaining aluminum overlay was removed from the affected fields, and testing resumed. Because the overlay is only a reliable switch if its effect on the card drops off steeply as its area is reduced, comparisons were made between each set of coverage. Reliability could then be confirmed if the difference between satisfying the stated confidence level and failing to satisfy occurred at a boundary between sets--that is, precisely after a portion of the overlay had been removed.

3.2.5 Testing Schedule

These are the steps taken for the experiments:

1. Construct the 2-region prototype RFID card
2. Mark fields and serial numbers of each region
3. Verify uncovered reading on RFID interrogator

4. Verify failure to read fully obscured card (both regions taped at 100% coverage)
5. Uncover both regions
6. Verify that coverage effects are temporary and reversible
7. Begin experimental taping: randomly select one of the 2 regions
8. Apply tape to respective region
9. Reset cycle count to 0
10. Record serial numbers of covered and uncovered regions
11. Mount card on conveyor, with motor set for rotation on pitch axis
12. Run for 1000 cycles, recording read results
13. Mount card on conveyor, with motor set for rotation on roll axis
14. Run for 1000 cycles, recording read results
15. Mount card on conveyor, with motor set for rotation on yaw axis
16. Run for 1000 cycles, recording read results
17. Conduct test of independence of the readings on the first region
18. Record p-value; flag if greater than confidence level
19. Shift overlays one position
20. Repeat cycling procedure
21. Continue experimental taping: randomly select one of the 2 regions
22. Randomly select an angle from half of unit circle; halve the overlay along angle
23. Repeat data recording for each of 3 axis, as described
24. Compare data with confidence threshold; continue collection until met
25. One threshold is met, record outcome
26. Run for additional confirmatory course of 1000 cycles
27. Perform final statistical analyses
28. Report test results in terms of hypotheses

3.3 Statistical Analyses

The test process was modeled using 2x2 contingency tables of outcomes, with the state of coverage on one dimension, and the interrogation result on the other. Such a table accurately represents each of the 4 field state combinations. In successive tables, the total surface area of the overlay is halved. To test the extent to which the availability of card data is affected by the detuning of the overlays, one inviting instrument would be a regression analysis.

Linear regressions are frequently applied in similar studies, where continuous data values are possible, but the binary outcomes of the card interrogation in this case made a logistic regression analysis most appropriate. A thorough explanation of the differences between the two, and the unique suitability of the latter in binary cases such as this one appears in Iowa State University's project Beyond Traditional Statistical Methods (Cook, Dixon, Duckworth, Kaiser, Koehler, Meeker, and Stephenson, 2001).

Given the independence of the card observations, logistic regression would indeed seem a fitting tool. The experiment proposed involves thousands of samples, and involves nothing that would apparently skew the error distribution.

> Just as with ordinary least squares regression we need some means of determining the significance of the estimates of the model parameters. We also need a means of assessing the fit, or lack of fit, of the logistic model. Inference for logistic regression is often based on the deviance (also known as the residual deviance). The deviance is twice the log-likelihood ratio statistic. The deviance for a logistic model can be likened to the residual sum of squares in ordinary least squares regression for the linear model. The smaller the deviance the better the fit of the logistic model. A large value for the deviance is an indication that there is a significant lack of fit for the logistic model and some other model may be more appropriate. (Cook, et al., 2001)

Asymptotically, the deviance has a χ^2 distribution. Therefore, to perform tests of hypotheses regarding the fit of the model the deviance is compared to the percentiles of a χ^2 distribution. The degrees of freedom is determined by the number of observations less the number of parameters estimated. Keep in mind that this is an asymptotic (large sample size) procedure and the P-values calculated using the χ^2 distribution are approximate. (Cook, et al., 2001)

The difference between the null deviance and the residual deviance represents the effect of adding the single explanatory variable to the logistic model. This is analogous to the change is the sum of squared residuals (sum of squares for error) in ordinary least squares regression. When an explanatory variable is added in ordinary least squares regression, the change in the sum of squares for error represents the amount of variability explained by that variable. The change in deviance in logistic regression can be compared to a χ^2 distribution to determine statistical significance. The degrees of freedom for the χ^2 is equal to the number of predictor variables added to the model, in this case, 1. Keep in mind that this test, like all the others, requires a large sample size and any results are approximate. (Cook, et al., 2001)

An alternative to the change in deviance for determining statistical significance of predictor variables in logistic regression is given by an approximate z-test statistic:

z= estimated parameter / standard error

Figure 12 Approximate Z-Test Statistic

This z-test statistic has an approximate standard normal distribution for large samples. For very large samples (another asymptotic result) the change in deviance and the square of the z-test statistic should give approximately the same value. (Cook, et al., 2001)

To prevent the inaccuracies that may arise from hand transcription and mathematical operations, the analyses of this experiment were run in the laboratory using the statistical language R. Data sets were collected directly into computer files and hashed with an error-detection code. Resulting figures and tables were machine generated using standard function libraries. No transcription errors were detected in the data.

Reputable RFID tag testing is ordinarily conducted at a 95% or 99% confidence level (Maniyan, Ghassemi, & Rahrovy, 2012). Given the high manufacturing tolerance of most tags, confidence at both levels can be regularly met by technologies used as designed, within reasonable environmental limits (Shahzad & Liu, 2012). Testing was conducted at the higher confidence interval, as it has been shown that in similar lab test protocols, the number of tag responses differs little from the number of read attempts for sampling sizes above 1000 (Qiao, Chen, & Li, 2013).

CHAPTER 4. RESULTS

4.1 Test 1: Independence

4.1.1 Preliminary Testing Overview

A baseline test was conducted with the card's data regions completely exposed. 1000 samples were taken in each of the 3 axial orientations, for a total of 3000 samples. With the baseline established, and proper operation of the reader equipment demonstrated, the next 3000 were taken, with the data regions completely obscured. Results were compared to the baseline. Then, to make certain that the suppression of the obscured fields had been temporary, and had not resulted in any lasting effect to the card, an additional 3000 samples were taken completely exposed. No functional anomalies were observed.

4.1.2 Direct Effect Test Overview

One of the two data fields was randomly selected for treatment in the direct effect test, which began with the fourth course, as shown in table 2. The selected field was completely obscured, while the remaining field was completely exposed. 1000 samples were taken in each of the 3 axial orientations, for a total of 3000 samples. The fifth course then proceeded in similar fashion with the coverage states exchanged, for an additional 3000 samples. Data were aggregated and compared against cycle count to obtain the total fault count.

It is considered a "transfer fault" if the reader fails to obtain data from an exposed region of the card, and a "blocking fault" if the reader obtains data from an obscured region. To follow are the totals, separated by configuration on their axis.

4.1.3 Data

4.1.3.1 Preliminary Testing

Table 1 Preliminary Test I Data

Course	Scan Total	Coverage[1]	Transfer Faults[2]	Blocking Faults[2]
1	3000	0,0	1 = (0+0+1)	-*NA*-
2	3000	1,1	-*NA*-	0 = (0+0+0)
3	3000	0,0	0 = (0+0+0)	-*NA*-

Note:

[1] 0: exposed, 1: concealed

[2] total is sum of faults on axes (roll+pitch+yaw)

4.1.3.2 Direct Effect Test

Table 2 Direct Effect Test I Data

Course	Scan Total	Coverage[1]	Transfer Faults[2]	Blocking Faults[2]
4	3000	0,1	0 = (0+0+0)	0 = (0+0+0)
5	3000	1,0	2 = (1+1+0)	0 = (0+0+0)

Note:

[1] 0: exposed, 1: concealed

[2] total is sum of faults on axes (roll+pitch+yaw)

4.1.4 Analysis

The data are visibly compelling even before statistical tools are used. At full data field coverage, not a single instance of blocking failure has been observed. The incidents of data transfer failure have demonstrated no statistically significant pattern, and remain within the advertised tolerance of an RFID card under normal operating conditions. Using statistical tools, the independence of the regions under test may be quantified.

As explained above, the statistical significance of a variable's deviation may be found by comparing it to a χ^2 distribution (Cook, et al., 2001). A test for independence was conducted on the relationship between the blocking faults of both the concealed region and the exposed region with respect to the state of coverage on the concealed region. This involves placing the sums of the faults and states on opposing axes of a matrix and feeding them into the χ^2 test. The regions' coverage is considered independent unless the test returns a p-value below α. The following resulted from R:

Table 3 Test for Independence of Data Fields

Data Region	χ^2 value	degrees of freedom	p-value
1	0.0007	1	0.9794
2	0.0007	1	0.9794

The input values for the second region were, of course, equal to the first but compared against the first region rather than the second. The output values were equal.

H0a (One data field will not depend upon the overlay coverage of another field.) has withstood the test, as its p-value is considerably higher than the boundary of .01. The null hypothesis is accepted.

Independence between data fields of the card has been determined.

4.1.5 Outcome

This hypothesis was put forth to test the first Research Question. Confirming it demonstrated that selective detuning is a feasible mechanism for independent selection of card data.

4.1.6 Further Investigation

For additional rigor, the test was given a second run, but this time to measure how the target region's state of coverage affected its own readability. The result indicated a strong dependency (with a p-value well below the .01 boundary). In other words, the overlay affects readability of its own data, but only its own data:

Table 4 Alternative Test for Independence

Data Region	χ^2 value	degrees of freedom	p-value
1	5988.009	1	<.001e-3
2	5988.009	1	<.001e-3

4.2 Test 2: Reliability

4.2.1 Preliminary Testing Overview

A baseline test was conducted with the card's data regions completely exposed. 1000 samples were taken in each of the 3 axial orientations, for a total of 3000 samples. With the baseline established, and proper operation of the reader equipment demonstrated, the next 3000 were taken, with the data regions completely obscured. Results were compared to the baseline. Then, to make certain that the suppression of the obscured fields had been temporary, and had not resulted in any lasting effect to the card, an additional 3000 samples were taken completely exposed. No functional anomalies were observed. See Data section of Test 1 for preliminary test data.

4.2.2 Direct Effect Test Overview

For the first testing course, a randomly selected data field was obscured except for 50% of the surface area of the overlay, which was removed along a randomly selected angle through its midpoint (as described in Methods). 1000 samples were taken in each of the 3 axial orientations, for a total of 3000 samples. It is considered a "blocking fault" if the reader obtains data from an obscured region. The number of such faults was compared against the threshold value of 30 (obtained by taking the number that is 1% of the total number of samples in the testing course). This number did not meet the threshold, so the test continued.

For the second testing course, the data field's overlay surface area was further reduced to 25% in another randomly selected portion. 1000 samples were taken in each of the 3 axial orientations, for a total of 3000 samples. The number of blocking faults was compared against the threshold value. This number met the threshold. The testing schedule called for a third course. If the trend continued through this confirmatory course, testing would halt.

For the third testing course, the data field's overlay surface area was further reduced to 12.5% along another randomly selected angle. 1000 samples were taken in each of the 3 axial orientations, for a total of 3000 samples. The number of blocking faults was compared against the threshold value. This number, too, met the threshold, so the tapering trend was confirmed and testing was halted.

4.2.3 Data

Table 5 Direct Effect Test II Data

Course	Scan Total	Coverage[1]	Transfer Faults[2]	Blocking Faults[2]
1	3000	.5	0 = (0+0+0)	0 = (0+0+0)
2	3000	.25	0 = (0+0+0)	1 = (1+0+0)
3	3000	.125	0 = (0+0+0)	3000 = (1000+1000+1000)

Note:

[1] percentage of surface area

[2] total is sum of faults on axes (roll+pitch+yaw)

4.2.4 Analysis

A binomial logistic regression is needed to visualize the transition of a data field from its exposed state to its concealed state. The result of its test signifies whether the effect should be seen as reliable, and the slope of the regression curve provides an illustration of how close to the binary ideal this physical implementation has come:

Table 6 Binary Logistic Regression Test for Reliability

Deviance Residuals				
Min.	1Q	Median	3Q	Max.
-6.7280	0.0000	0.0000	0.0008	0.0365
Intercept Coefficients				
Estimate	Std. Error	z value		
22.633	1.732	13.07		
Coverage				
Estimate	Std. Error	z value		Pr(>|z|)
-61.279	4.899	-12.51		<.001e-3

When the read outcomes of testing at all coverage levels are aggregated and plotted, a sharp transition becomes visible between 25% and 50% coverage. The logistic regression curve follows its characteristic S-shaped pattern, but with a steep slope in the transition region:

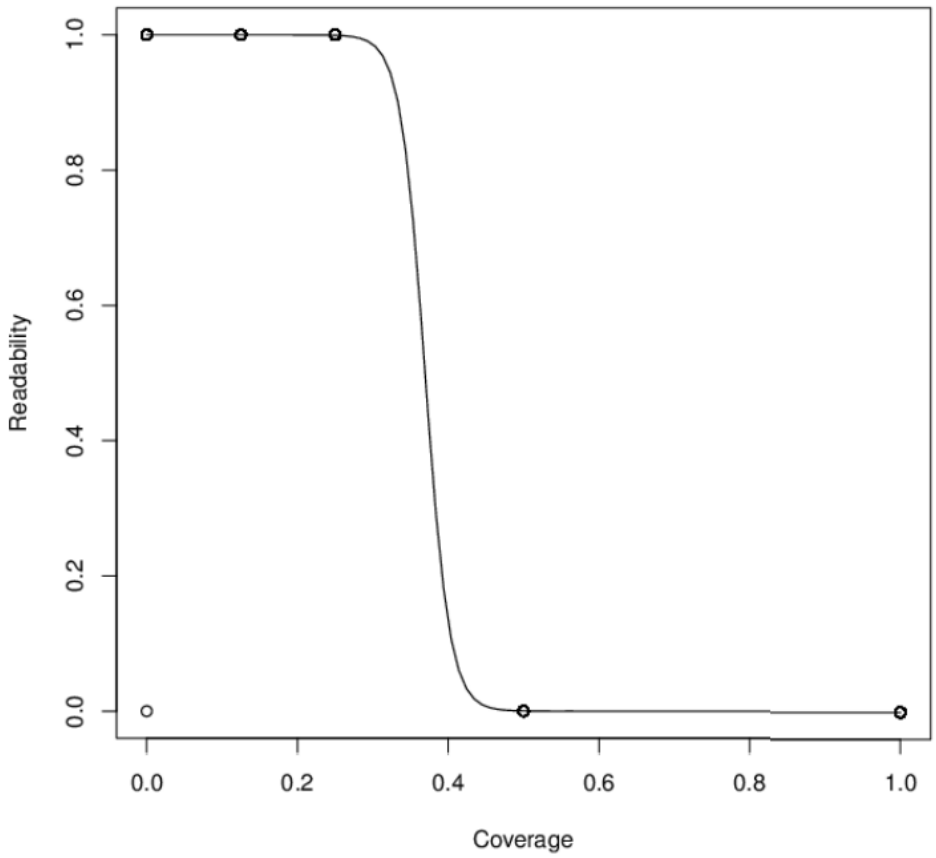

Figure 13 Logistic Regression Curve of Overlay Effect

This indicates that the card has succeeded in separating clearly the distinction between a concealed region and an exposed region. Its behavior is as close to binary as practical, and tends toward the shape of a square wave.

H0b (The effect of the overlay will not show a predictable decline as its coverage is reduced.) has been rejected as its probability is considerably lower than the boundary of .01.

H2 (The effect of the overlay will show a predictable decline as its coverage is reduced.) has been confirmed.

The success rate fell from 100% to 99.9% as coverage was reduced from 50% to 25%, yet from 99.9% to 0% when coverage was reduced from 25% to 12.5%. The reliability of the coverage effect on the data field readability has been empirically demonstrated.

4.2.5 Outcome

This hypothesis was put forth to test the second Research Question. Confirming it demonstrated that selective detuning operates reliably enough to be practical even in a user landscape where the coverage area is likely to be inconsistently applied, due to human variation and error.

4.2.6 Further Investigation

Given how the antenna pattern geometry varies in different directions, it seems reasonable to suspect that orientation of the overlay on the card data region would become highly influential near the surface area transition. For this reason, several other orientations of 25% surface area were tried, and eventually one was found that resulted in a blocking fault, but only a single blocking fault in the entire course:

Table 7 Alternative Orientation Test

Course	Scan Total	Coverage[1]	Transfer Faults[2]	Blocking Faults[2]
4	3000	.25	0 = (0+0+0)	1 = (1,0,0)

Note:

[1] percentage of surface area

[2] total is sum of faults on axes (roll+pitch+yaw)

The same attempts were made at 12.5% coverage, but no such orientation was found. The user may be confident that coverage greater than half of the region will completely prevent reading, and coverage less than an eighth of the region will leave it completely readable.

CHAPTER 5. CONCLUSIONS

5.1 Research Question I

The following line of investigation began with the first Research Question: "Is selective detuning a feasible mechanism for independent selection of RFID card data?"

From this came hypothesis H0a:
"Access to the data of a given field will not depend upon the overlay coverage of a field other than its own."

This hypothesis has been tested experimentally and accepted.

Building a card with multiple sensing regions is simple and affordable, as it is with existing RFID card models. Selecting regions with a readily available material such as aluminum tape works decisively to select card data, provided that over 50% of the region is covered. It is effective even when the user is imprecise and the environmental effects arduous enough to damage the overlay. Data fields are not significantly affected by changes to the coverage status of their neighbors. The feasibility of the overlay method has been demonstrated.

5.2 Research Question II

The following line of investigation began with the second Research Question: "Can a design for selective RFID detuning operate reliably enough to be practical?"

From this came the second Hypothesis:
"The effect of the overlay will decline reliably as its coverage is reduced in the tested region."

This hypothesis has been tested experimentally and accepted.

The design tested here exhibited few operating failures. Data intended for disclosure was successfully read as often, on average, as with existing RFID cards. Data intended for concealment was successfully kept from being read in every instance where overlay coverage of the data region was between 50% and 100%. Excess overlay material was not a source of interference, provided that it caused no more than 25% coverage. Subject to statistical tests , this proved to be a reliable design, both in terms of the independence of data fields and the responsiveness of any given data field.

5.3 Discussion

RFID card technology is frequently billed as an upgrade to printed cards, and a likely if not inevitable successor. It seems reasonable that if a device is called an "upgrade", it offers at least the functionality of its predecessor. By making the granular selection of data fields impossible, popular RFID cards have shown at least one way in which they represent a decline in value to the user. It is a difference that has been felt, and is quantifiably significant to them, such that they are willing to shape their behavior accordingly (Clement et al., 2012).The model illustrated here restores selection function, and allows it to happen by a familiar method that closely parallels what had been done to conceal fields on printed media.

Owing to its simple, affordable design, the model card is a practical solution to the needs of a large user population. It does not suffer from the granularity limitations of older RFID cards, nor the durability limitations of mechanically switched cards, nor the

cost barriers of processor-based cards. It is ready for mass production and distribution. It is easily replaced if lost or damaged. Its size is comparable to the form factor of existing cards, and it may be used in the manner of existing cards. It simply adds to them the new functionality of non-contact RFID technology. The switching mechanism is of an importance that grows in proportion to public concern over the unauthorized acquisition and use of personal information from identification cards. RFID allows data to be acquired from a distance, and without any user notification, so a means to toggle card access is immediately attractive. Refining that access down to the level of specific data fields adds a flexibility to the experience that was not available in the comprehensive card shielding solution used in established cards.

It was expected that a novel design with independent switching regions of this type could be constructed. Early modeling suggested that the electromagnetic compatibility requirements could be met using the antenna geometries described here for the card. Experimentally, it was found that independence had indeed been demonstrated with each data field against the other, consistently enough to meet the threshold of statistical hypothesis testing. While internal coupling of charge would have been a problem for various other designs outside this study's scope, it has been successfully prevented here by the unique approach used. The extent to which the data fields have been made independent is sufficient to support the claim that what is done to reveal or conceal one field shall not have an effect on any other fields.

As the reliability of RFID read operations on established card designs is very high, it was expected that the reliability of the prototype cards during normal reading would fare no worse in test. This was indeed confirmed. It was the prospect of achieving similarly high likelihood of blocking operations that made the experiment following Research Question II so inviting. As discussed earlier, blocking methods involving detuning can exhibit very high reliability. Since the prototype was constructed to exacting specifications and given preliminary testing that presented no surprises, it was expected that either it would perform reliably during the long formal sessions of the test or some

remarkable anomaly would become apparent. No anomaly was recorded. Blocking performance not only met but exceeded that of read performance, suggesting that in applications involving longer periods of recording and larger numbers of users the overlays would be as reliable as comprehensive card shielding.

The review of literature pertinent to RFID began in the mid-1990s. All material was taken into account, and all published in 2000 or later was considered for citation here. Articles from a variety of the most popular academic and public news sources were read in search of ideas for how the data field granularity issue was being addressed. The catalogs of major RFID manufacturers were regularly reviewed also, as their products were being used in earlier research projects. For this particular project, the question of whether detuning overlays had been presented as a solution for independent field selection was specifically posed using Purdue's library search facilities--some of the most powerful in the nation. The US Patent and Trade Office was likewise searched comprehensively for claims to any invention that might sound similar enough in description to indicate that it was no longer a novel approach (see Appendix for details). As nothing of this nature was found, it is introduced here. Other researchers clearly knew that detuning without complete shielding was possible, but did not present it as a means of data field selection. As far as determined, the description presented above is original.

5.3.1 A Review of the Testing Protocol

As the experimental portion of this work was being prepared, an early and obvious question concerned what are the factors most influential in the success and failure of ordinary RFID read operations. In the Experiment Design appears the complete list of factors that were controlled, but in practical use there are two that tend to dominate all others. The first is distance between the card and reader. As explained, a proximity card is only usable on the order of a few meters during normal operation. It was clear that during the experiment the card would need to be close enough to the reader to accurately represent such a span. Moreover, it would need to approach the reader while it is

transmitting at a continuous duty cycle, and from a distance. It would need to move smoothly through the full range of space at a speed slow enough to allow any area of weakness in the card or the radiation pattern to become observable.

The second dominant factor is card orientation. As detailed under the Data Collection section of Chapter 3, the radiation pattern of the antennas used in RFID cards (both the prototype design and its commercial predecessors) is not equal in all spherical directions. In fact, the differences can be profound enough that, for example, a user might find a card held in orientation perpendicular to the panel antenna commonly used with readers is not readable, even on the order of a few centimeters away, until the card is rotated in hand. This brings the elements of both antennas closer to parallel, and closer to coupling for maximum energy transfer. In order to test card performance in terms of independence or reliability, it would first be necessary to control for how the card's orientation varies during common use. This is why the test apparatus comprises a separate motorized mount that sweeps each pass of the card through its entire range of axial orientations. It was chosen as a practical way of proving that no superior card position had been overlooked during the course of testing.

The mechanical gantry illustrated in figure 11 had to reliably support the mounted shuttle and rotator over many cycles as they that conveyed the card into and out from the read zone. They had a simple path to travel, but plenty of ways to glitch if assembled without regard for detail. The power supply driving them was connected to a conditioned municipal source, and rectified to direct current. Batteries were avoided, as their voltage would vary over time as they discharged. The gears and bearings were housed in fully enclosed boxes to keep them resistant to dust and debris. The timing of the system was microcontrolled, not because the degree of precision this offers was required for the card passes, but because the ease by which feedback may be used here for keeping the parts synchronized is great, while the cost of simple microcontroller boards is low.

As construction of the experimental system was happening, a great deal of testing was done on the possible detuning effects of the motors, hardware, and other parts of the system. The focus of testing was the overlay, and care was taken to ensure that no other parts involved confounded the results. A transistorized dip meter was employed to measure the absorption by the card's antennas of RF energy on the fixed frequency of operation, 13.56MHz. It was quickly determined how far from the antennas other conductive materials would have to be in order to prevent interference with the overlay. System hardware interference was reduced below detectable levels by increasing the parts' distance from the antenna portions. A spacing was chosen to promote compatibility between the moving parts and the electromagnetic fields near them.

The practical efficacy of this card has been demonstrated in a controlled setting. It beckons further studies that might include test replications. If experiments related to this work are undertaken in the future, they might be conducted differently, with some of these points considered:

To the extent they are available, university research facilities may be an expedient and helpful source of existing test equipment. There is much common preparation in all such experiments, and energy could have been saved if the space had been available already. Instead, it had to be prepared for RFID testing and then the specifics of this paper. Future investigators are encouraged to collaborate with institutions of higher education that might already have space designated for this type of RF testing, or be planning the establishment of labs for such a purpose. Often this is not advertised outside the school, or even to other colleges on the same campus.

The capacitive switching model described in the Delimitations has in fact been prototyped, but could not be included in the testing here because its thickness was too great for use as an RFID card, and thus too large for the test system of the Methods. While it brings perhaps too much material to include in the same dissertation, this method of switching is the natural successor to the detuning methods described here. If a suitable

fabrication facility could have been involved in the preparation of prototypes, there could have been included a comparison between the two card technologies, and illustrative examples of how they differ. For the time being, it must do that the proof of concept has been made. The overlay scheme used in it would only be given greater precision and flexibility in a capacitive system. More work done to miniaturize its components is desired.

More involvement from people is needed in order to make this RFID solution demonstrably relevant and effective in terms of a practical deployment. Matters as seemingly small as the feel and appearance of the overlays can have a major impact on results in the field. In line with the studies mentioned in the Literature Review, more is needed for interdisciplinary work here. Many questions about personal values, routine, and propriety can be answered only by those whose lives are affected by the technology change. Since every new device embodies a paradigm, it is important that users be observed and surveyed over a long term to see whether this paradigm is one in which they are comfortable. Trends shift according to factors that card engineering cannot address, such as media coverage of the topics, or prevailing government and regulatory stance. It would seem favorable to include research on human subjects in more ID work, which is after all directly relevant to personnel. Carrying and manipulating cards is a process much less invasive in a subject's life than many proposals that come before an institution review board. This factor is useful in securing approval for it, provided a direct and articulate researcher can drive those differences home.

5.3.2 Additional Laboratory Observations

Though separate from the observations following the Research Questions, these points were illustrated during the experiments, and seem salient enough to include:

- Consistent with industry claims, the RFID card and reader performed with high reliability before overlay technology was introduced, exhibiting on average fewer than one read error per thousand attempts (over 99.9% reliability).
- The general effectiveness of detuning conductors was visible immediately and strikingly throughout testing. Not a single error arose in the read blocking at any state of coverage over 50%, even after many thousands of iterations.
- The effects of the aluminum tape were found to be temporary and completely reversible, having no lingering effect on the card between applications when tested for independence at 99% confidence.

5.3.3 Exclusions and Limitations

The purpose of this dissertation is not to test all of the factors that make traditional plastic cards attractive, but to test the particular mechanism outlined. The other factors, though vital, are considered to have been adequately tested by the governing agencies that deployed them, and proven over many decades of public use. Adding RFID technology to cards of familiar composition and size eases the transition, which helps to explain why electronic cards are already used as national identification in Hong Kong, Malaysia, Estonia, Finland, Belgium, Portugal, and Spain (Nogueira & Greis, 2009).

As this was a technological investigation, it did not offer testing of human factors. This remains a vital aspect of any successful deployment. With the model cards now available and shown to function as claimed, those inclined to conduct research on their usability would find a prime invitation. It would seem helpful if there could be studies in the future that address public eagerness or hesitance to use RFID cards regularly in this

way, ease of data field selection using common tape and overlays, the indirect benefits of information separation, and so forth. New technologies cannot achieve widespread acceptance unless they are introduced at a time conducive to it, and in a cultural landscape where a great variety of people will find the solution preferable. At the least, it is needed that many real users are exposed to overlay selection cards and given a chance to show researchers any practical objections to implementation might have been overlooked.

5.4 Recommendations

Readers will note that in the course of this experiment, some findings have appeared that would have implications for those involved in management of an RFID deployment, and others that would have implications for those in research and development. Below are some of the things to keep in mind when taking the RFID solution of this dissertation out of the laboratory and into popular use, as well as the things that follow from the particular work done in this technology, in terms of its future research potential.

5.4.1 Concerning Technology Deployments

5.4.1.1 Uniquely Identifying People

RFID is used, in this context, for distinguishing documents such as cards, from a distance. It is not directly involved in distinguishing people. For that, some unique human factors would need to be measured and stored in the RFID card. This is the realm of biometrics, which is a separate but often connected discipline. For long, the photograph on the card along with simple details such as height and eye color have been used to tie the card to its bearer. It is of utmost importance that plans for an RFID-enabled personnel solution include at least as much effort. If it becomes possible for another party to physically obtain the card, then the privacy limiting mechanisms discussed in earlier

chapters may be disabled by him just as readily as by the legitimate owner. If the biometric factors do not uniquely and exclusively tie the card to its owner, then it may become possible for others to use the card for impersonation. As discussed in the delimitations, such matters are beyond the scope of this dissertation. They nonetheless must be recognized and dealt with if its findings are to be applied practically.

5.4.1.2 Large-Scale Applications

Any RFID technology for personnel requires the backing of legislation if it is to be deployed on the scale of a state or country. Though policy issues form another matter beyond scope, these conclusions and recommendations might still serve to prepare those who wish to propose or defend policy changes. RFID-enabled driver's license cards are already in use in several states (DMV.org, 2015) and card field selection by means of overlays has been shown to work well (Clement et al., 2012). The discussion might now move toward tailoring the prototype card of this dissertation to the exact specifications required for the state or national entity that would use it. Those involved in the design and production of such technologies could be bolstered greatly by the support of legislative bodies that commit to the use of their results.

Among the primary specifications to be made there is the number of fields needed for a specific deployment. This will affect the number of switching regions into which the card space will be divided, and thus the size of each region. Manufacturers such as Murata have produced antennas as small as 3.2mm²--small enough to fit inside the "d" of an Indiana state driver's license, and clearly smaller than any card region a user would need to cover (Swedberg, 2012). Its .7mm thickness is less than the 1mm maximum listed above in Design Factors as well, so there is no apparent technological barrier to resizing the model fields accordingly. This is simply one of the factors that planners will need to recognize and specify early.

The trend of replacing a printed card with an electronic card as the driver's license has expanded steadily, not only in the United States, but worldwide. It has included, among others, El Salvador in the late 1990s, several states of India in 2003, Japan in 2007, Morocco in 2007, Mexico in 2007, Indonesia in 2009, Australia in 2010, Croatia in 2013, France in 2013, and Ireland in 2013. Several of these such as Japan, Morocco, and Indonesia were RFID-enabled cards (Stoltz, 2014). Above in the Literature Review, "enhanced" driver's license cards were discussed. RFID is considered a fundamental technology for these cards (U.S. Customs and Border Protection, 2014). At the time when this section was written, the states of Washington, Vermont, New York, and Michigan had fully implemented EDL cards. Arizona and Texas were in progress (DMV.org, 2015). It is strongly recommended that interested parties in these states consider how selection mechanisms will figure in the future of such cards.

5.4.1.3 Ramifications of a Detuning Approach

Those planning to propose a deployment based on the findings here might wish to mention some of the facts that make it especially attractive:

- The presented shielding method works even on RFID cards have no die, such as those commonly used for electronic article surveillance in stores, etc. The 8.2MHz LC tank circuit sticker used for loss prevention is a good example.
- The foil works on either side of the card, so it's possible to obscure the RFID replies (by taping the back of the card), while leaving the front visible.
- The foil prevents not only read operations, but also write operations, protecting the user against attempts to alter or destroy card data.

To ease the transition to a detunable card, users should be assured that it presents no drastic change in usability. Its look, feel, and performance make it resemble one of the existing RFID-enabled driver's license cards. Those that would prefer to use it as such are free to do so. Some will not even realize that there is any change in the detunable design.

Those that wish to use the selection feature, though, will be able to do so in much the same way they did with the old print cards. The only difference is that instead of selecting a visibly opaque tape for cover, they will be selecting an electromagnetically opaque tape (or tape alternative overlay such as film, sleeve, bar, etc.) Common aluminum tape is sold near masking tape in hardware stores across the country. No sophisticated electronic accessories are needed to enable the feature.

User education will be of importance here, as it is not possible for the card to discern the will of those holding it. It will need to be established early that there is a difference in selectivity between keeping the card in an enclosed sleeve (which renders it completely unreadable until removed), and obscuring only particular regions of the card (which renders only those regions unreadable). All the usual warnings concerning electro-static discharge, extreme temperatures, and strong magnetic fields will need to be included when the card is introduced. This will not be difficult, as it is nearly identical to the warnings for common chip-and-PIN smart cards issued for credit and debit, etc. Finally, it is advisable to remind the user that because the print and the RF emissions of the card are not drawn from one common data store, there does exist the possibility that, in the case of accident or tampering, they might disagree. As the magnetic stripe of a card must be verified against its print, so must the RFID output against its print, and against any other means of storing the data in such a card (recall earlier caveats from Inviting the Card Overlay Solution).

5.4.2 Concerning Research and Development

Perhaps the most important recommendation to other researchers is that they take the results of this work into experiments involving practical users in realistic environments. This could be an excellent opportunity for specialists in the humanities to prepare work similar to what Clement et al. did in their 2012 study of identification cards. Events such as conferences and workshops provide ready groups of attendants who would be issued identification cards anyway. Such cards could be modified for selective detuning, and developments during the event deliberately chosen as an incentive to users for selection. These attendants could later be surveyed on the experience, to evaluate their acceptance of the model and any usability concerns that might have arisen.

College campuses are another inviting test bed for ID card technologies. Many have huge student, staff, and faculty populations who will be attending the institution on the order of years, making a longitudinal study more practical. Questions of how the card might wear over time could be answered empirically by following marked users over time. Questions of whether users understand the value of the personal data selection could be answered by brief and regular online surveys. Playful contests might be introduced as an incentive for the user to apply the selection mechanism to prevent mock antagonists from tracking their activity or obtaining their private data. Those who manage to stay safe while still passing legitimate transactional data (such as student ID number, etc.) might become eligible for gift drawings, etc. Those "victims" whose private data are successfully "stolen" might receive an e-mail message warning them about the threat of real antagonists and fraud.

As mentioned often in this paper, the public has had an ambivalent relationship with RFID, wary of it even as they show interest in its offerings. Some privacy experts studying their reaction summarize it in this way:

> Research indicates consumers are willing to make certain tradeoffs of their privacy for benefits such as convenience... but individuals want to know when there is a potential that their privacy might be at risk, and they want to retain control of the choice to change that level of risk. (Schenke, 2010).

If users are to be trusted in accepting and using a system as designed, inspiring their confidence in it is of tremendous importance, regardless of whether the anticipated problems manifest. The state of California, for instance, had planned to roll out a new driver's license card in kind with Arizona and Texas, but in 2013 suspended legislation to put RFID technology in it due to complaints from privacy groups (Kravets, 2013). This is where technology ambassadors have a chance to resolve such conflict in other states and countries.

The method described here places the privacy tool in the users' hands, which not only helps the issuing entity illustrate its commitment to user protection, but also might help reduce its liability. More attention from researchers in fields such as Communication, Sociology and Anthropology is highly recommended, as there appear to be many opportunities for study of changing attitudes surrounding this technology.

While the testing reported here dealt with a hardware-level solution that is usable even with passive RFID device, a small step from it takes related research into smart card technology, and the prospect of using the conductive overlays as a means of directly manipulating the settings of an onboard computer. The earlier discussion of capacitive switching outlines how this would become possible. To the user, the use of overlays would be no different, but would control a larger set of possible functions, including anything within the capabilities of cards containing processing circuitry.

5.4.2.1 Linking Data Fields

It is not necessary, with this model, to use only one card per user. Multiple cards may be produced, linking any of desired fields of the user's record, and excluding from a particular card's storage all other fields. Data set relations is a separate topic, but deserves brief mention here. It is important in cases where a card would be physically passed, and the privacy overlay could be removed. For example, in contexts needing age verification or name verification, this could allow it even at the high speed of RFID processing, without risk that additional information be obtained by manipulating the card. The detuning approach cooperates with a variety of data isolation strategies at the hardware level, and so system architects planning for a deployment would do well to consider exactly which data fields are desirable for which cards, and in which contexts.

The discussion of wireless cards for identification is not complete without a discussion of the databases against which the card data are to be compared. In such a system, it must be clearly delineated which data should reside on the card and which should reside in the database, related to the card by some unique identifier. In deployments involving drivers' license cards over the past two decades, it has been common for the RFID component to release only the unique identifier. A computer network relates this identifier to as many user fields as desired. Database management is beyond the scope of the discussion here, but it must be taken into account for a practical case, as cards that provide individual field selection call for a different engineering philosophy than is currently in use.

RFID-enabled driver's license cards from Washington, to cite one representative example, are used to poll a central database of biometric data (Washington State Department of Licensing, 2015). Without this, the wireless feature of the card is not complete as a form of personal identification. It is really only self-identification of the card. Exploring how many fields belong in the database and on the card, as well as how the keys tying them should be exchanged is clearly worth recommendation. The overlay

solution presented above provides a means to select and disclose such keys, but without the cooperation of those entities that control the database, the purpose of the overlays could be neglected during implementation.

5.4.2.2 Other Prospects

Some suggestions for further research in overlay selection technology include

- Adding to RFID the type of challenge/response interactions popular in encrypted smart cards. This could unite the technology of both nicely, but give the user the ability to control its operation with overlays.
- Experimenting with fields specifically shaped for pinching with a fingertip. Above it was discussed how pinch switches can be quite handy to enable reading of a card that is handled often (Huber, 2012). Mechanical switches are thick and prone to damage, but surface capacitor plates that sense the proximity of a finger may be as thin as the card.
- Using capacitive pads to allow user selection of PINs and such. Ordinarily, such cards are programmed with an external unit, but if several configurations were known to be useful in the future, they could all be programmed, and the user could later select between them by using the pads as a simplified wireless keyboard.

5.5 Summary

A novel RFID card design has been introduced to provide a data selection function through the use of conductive overlays. The mechanism undergirding it has been validated through laboratory tests and shown highly reliable. Its effects are temporary and reversible, requiring no external electronics to perform selection. Users interact with it through familiar, intuitive methods. Its composition and dimensions are as familiar as in existing cards, allowing it to be carried in the same fashion. This is important, as many civil functions call for personnel identification, and the license-sized plastic card has become an unofficial standard form of ID. Radiofrequency identification has been used with increasing popularity in this and many other identity documents. The user can retain discretion over whether the wireless communication features of the card are enabled, and for which fields. It is a technology platform suitable for innovation.

The model design offers distinct advantages over existing RFID deployments for personnel identification. It extends the functionality of traditional printed cards and empowers the user to better limit unauthorized disclosure of personal data. Granular selection of card data fields is possible with this design, which was not possible with the RFID cards that preceded it. This brings the prospect of technologies to follow, and implementation at the large community level. Many of the concerns that have held back other identification initiatives have been addressed here, with explanations of how the new design could bring remedy. A detailed explanation of the experiments was given, as an invitation to others that might perform related testing. Several opportunities for further research and application of the mechanism were discussed.

REFERENCES

REFERENCES

Abdullah, A.K. (2004, October 8). Protecting Your Good Name: Identity Theft and its Prevention. *Proceedings of the 1st Annual Conference on Information Security Curriculum Development*, pp. 102-106. Retrieved from http://dl.acm.org/ft_gateway.cfm?id=1059547

Albrecht, K. (2008, August 21). How RFID tags could be used to track unsuspecting people. *Scientific American*. Retrieved from http://www.scientificamerican.com/article.cfm?id=how-rfid-tags-could-be-used

Amer, S.H. & Hamilton, J.A. (2008, April 14). Understanding Security Architecture. *Proceedings of the 2008 Spring Simulation Multiconference*, pp. 335-342. Retrieved from http://dl.acm.org/citation.cfm?id=1400596

American Civil Liberties Union. (December, 2007). *Washington State Enhanced Driver's Licenses vs. U.S. Passports - Radio Frequency Emitting IDs and Your Privacy*. Retrieved from https://www.aclu-wa.org/sites/default/files/attachments/EDLvPassport_12_07.pdf

Authoritative Dictionary of IEEE Standards Terms, Seventh Edition. (2007). Institute of Electrical and Electronics Engineers. Retrieved from http://ieeexplore.ieee.org//xpls/abs_all.jsp?arnumber=4116787

Backes, G., Becker, R. C., & Cornett, A. (2014). *U.S. Patent No. 8,763,893*. Washington, DC: U.S. Patent and Trademark Office.

Bidinosti, C. P. & Hayden, M. E. (2008, October 29). Selective Passive Shielding and the Faraday Bracelet. *Applied Physics Letters, vol. 93 (174102)*. Retrieved from http://link.aip.org/link/doi/10.1063/1.2998607

Bouchard, O. (2014). *U.S. Patent No. 8,746,575*. Washington, DC: U.S. Patent and Trademark Office.

Bove, J. M. (2012). *U.S. Patent No. 8,111,160*. Washington, DC: U.S. Patent and Trademark Office.

Brazy, D. (2010, May 4). Ariz. College to Position Sensors to Check Class Attendance. *The Badger Herald*. Retrieved from http://badgerherald.com/news/2010/05/04/ariz_college_to_posi.php

Brookes, T. (2010). RFID and Privacy. *UK RFID*. Retrieved from http://ukrfid.innoware.co.uk/rfid_systems/rfid_privacy

Clement, A., McPhail, B., Smith, K.L., & Ferenbok, J. (2012, August 12). Probing, Mocking and Prototyping: Participatory approaches to identity infrastructuring *Proceedings of the 12th Participatory Design Conference: Research Papers - vol. 1*, pp. 21-30. Retrieved from http://dl.acm.org/citation.cfm?id=2347639

Coiro Sr., M. A., Miller, S. J., & Schupsky, T. (2012). *U.S. Patent No. 8,161,910*. Washington, DC: U.S. Patent and Trademark Office.

Cook, D., Dixon, P., Duckworth, W. M., Kaiser, M. S., Koehler, K., Meeker, W. Q., & Stephenson, W. R. (2001, February 7). Binary Response and Logistic Regression Analysis. *Iowa State University NSF/ILI project Beyond Traditional Statistical Methods*, ch. 3. Retrieved from http://www.stat.wisc.edu/~mchung/teaching/MIA/reading/GLM.logistic.Rpackage.pdf

Cram, Douglas. (2014). *RFID Technologies - RFID 101* [Flexible RFID card antenna inlay illustration]. Retrieved from http://www.tresrfsolutions.com/AFA_RFID101.pptx

DMV.org. (2015). *Passport Card & Enhanced Driver License*. Retrieved from http://www.dmv.org/driving-abroad/passport-license.php#Enhanced-Drivers-License-EDL

Douglass, M. (2006). *U.S. Patent No. 7,004,385*. Washington, DC: U.S. Patent and Trademark Office.

Douglass, M. (2007). *U.S. Patent No. 7,284,692*. Washington, DC: U.S. Patent and Trademark Office.

Douglass, M. (2009). *U.S. Patent No. 7,584,885*. Washington, DC: U.S. Patent and Trademark Office.

Galloway, J. (2010, April 19). Delusions, The Legislature and an Implanted Microchip. *The Atlanta Journal-Constitution*. Retrieved from http://blogs.ajc.com/political-insider-jim-galloway/2010/04/19/delusions-the-legislature-and-an-implanted-microchip/

Garfinkel, S.L., Juels, A., & Pappu, R. (2005). RFID privacy: an overview of problems and proposed solutions. *IEEE Security & Privacy, 3(3)*. Retrieved from http://simson.net/clips/academic/2005.IEEE.RFID.pdf

Gertz, B. (2008, March 26). Outsourced Passports Netting Govt. Profits, Risking National Security. *The Washington Times*. Retrieved from http://www.washingtontimes.com/news/2008/mar/26/outsourced-passports-netting-govt-profit-56284974/

Glossary of Common Cybersecurity Terminology. (n.d.). National Initiative for Cybersecurity Careers and Studies. Retrieved April 3, 2014, from http://niccs.us-cert.gov/glossary

Glossary of RFID Terms. (2014). RFID Journal. Retrieved from http://www.rfidjournal.com/site/glossary-of-terms

Greenblatt, A. (2010, April 15). Lawmakers Are Working on Anti-Brain-Chip Bill. *National Public Radio, All Tech Considered*. Retrieved from http://www.npr.org/blogs/alltechconsidered/2010/04/15/126023516/breathe-easy--ga--lawmakers-are-working-on-anti-brain-chip-bill

Gregorio, J. (2009, November 27). *CCD*. Retrieved from http://bitworking.org/news/2009/11/ccd

GS1 EPCglobal. (2013). *EPC Tag Data Standard 1.7*. Retrieved from http://www.gs1.org/gsmp/kc/epcglobal/tds

GS1.EPCglobal Gen2. (2013). *EPC Radio-Frequency Identity Protocols Generation-2 UHF RFID*. Retrieved from http://www.gs1.org/gsmp/kc/epcglobal/uhfc1g2

Haddock, R. M. (2014). *U.S. Patent No. 8,820,639*. Washington, DC: U.S. Patent and Trademark Office.

Hammerschmidt, C. (2008, April 1). NXP RFID encryption cracked. *EE Times*. Retrieved from http://www.eetimes.com/electronics-news/4197848/NXP-RFID-encryption-cracked

Hardgrave, B. C. & Miller, R. (2006, February). *The Myths and Realities of RFID*. Information Technology Research Institute, University of Arkansas. Retrieved from http://rfid.uark.edu/papers/ITRI-WP067-0306.pdf

Heim, K. (2008, March 31). UW Team Researches a Future Filled with RFID Chips. *The Seattle Times*. Retrieved from http://seattletimes.com/html/businesstechnology/2004316708_rfid31.html

Herrmann, S. (Ed.). (2007, May 25). Wi-fi and RFID used for tracking. *BBC News*. Retrieved from http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/6691139.stm

HID Global Corporation. (2014). [Product description of 293/296 SIO Solution for MIFARE DESFire EV1 + LEGIC prime 1024]. Retrieved from http://www.hidglobal.com/products/cards-and-credentials/legic/legic-prime-1024

HID Global Corporation. (2014). [13.56MHz physical card characteristics]. Retrieved from http://www.hidglobal.com/sites/hidglobal.com/files/resource_files/d00529-e.5-13.56- mhz-physical-access-htog-en_1.pdf

Huber, B. R. (2012, February 17). No more virtual pickpocketing of credit cards, thanks to new tap and pay technology. *University of Pittsburgh EurekAlert*. Retrieved from http://www.eurekalert.org/pub_releases/2012-02/uop-nmv021712.php

Hutzler, R., Nguyen, S. N., Smith IV, N. J., & Zimmerman, T. G. (2014). *U.S. Patent No. 8,823,497*. Washington, DC: U.S. Patent and Trademark Office.

ISO/IEC 15693. (2010). *Identification Cards - Contactless Integrated Circuit Cards - Vicinity Cards*. Retrieved from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=39694

ISO/IEC 14443. (2008). *Identification Cards - Contactless Integrated Circuit Cards - Proximity Cards*. Retrieved from http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=39693

Jei, D. G. & Lee, Y. H. (2008). *U.S. Patent No. 7,374,100*. Washington, DC: U.S. Patent and Trademark Office.

Johnson, R. C. (2008, May 14). Testbed Streamlines RFID Development. *EE Times*. Retrieved from http://www.eetimes.com/electronics-products/sensors-tranducers/4104243/Testbed-streamlines-RFID-development

Jones, M. H. (2014). *U.S. Patent No. 8,777,727*. Washington, DC: U.S. Patent and Trademark Office.

Juels, A., Rivest, R. L., & Szydlo, M. (2003, October 27). The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In V. Atluri, ed. *Proceedings of the 8th ACM Conference on Computer and Communications Security*, pp. 103-111. Retrieved from http://www.emc.com/emc-plus/rsa-labs/staff-associates/the-blocker-tag.htm

Kargl, W. & Sbuell, R. (2011). *U.S. Patent No. 7,912,430*. Washington, DC: U.S. Patent and Trademark Office.

Karjoth, G., & Moskowitz, P.A. (2005, November 7). Disabling RFID Tags with Visible Confirmation: Clipped Tags Are Silenced. *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, pp. 27-30. Retrieved from http://dl.acm.org/citation.cfm?id=1102205

Kim, W. K. (2011) *U.S. Patent No. 7,909,258*. Washington, DC: U.S. Patent and Trademark Office.

Kim, M. J. (2014). *U.S. Patent No. 8,816,819*. Washington, DC: U.S. Patent and Trademark Office.

Koh, W. H. & Ho, J. (2009). *U.S. Patent No. 7,564,359*. Washington, DC: U.S. Patent and Trademark Office.

Koscher, K., Juels, A., Kohno, T., & Brajkovic, V. (2009, November 9). EPC RFID Tags in Security Applications: Passport Cards, Enhanced Drivers Licenses, and Beyond. *Proceedings of the 16th ACM Conference on Computer and Communications Security*, pp. 33-42. Retrieved from http://dl.acm.org/citation.cfm?id=1653668

Koyama, J. (2010). *U.S. Patent No. 7,663,473*. Washington, DC: U.S. Patent and Trademark Office.

Koyama, J. (2010). *U.S. Patent No. 7,666,722*. Washington, DC: U.S. Patent and Trademark Office.

Koyama, J., Abe, H., Yukawa, M., Iwaki, Y., & Yamazaki, S. (2010) *U.S. Patent No. 7,795,617*. Washington, DC: U.S. Patent and Trademark Office.

Kravets, D. (2013, September 3). California Abruptly Drops Plan to Implant RFID Chips in Driver's Licenses. *Wired Magazine*. Retrieved from https://www.wired.com/2013/09/drivers-license-rfid-chips/

Krisch, A. (2007, December 5). RFID usage and informed consent - Using and removing of RFID functionality. *European Digital Rights Papers*. Retrieved from http://www.edri.org/docs/EDRi_RFID_Informed_Consent_published.pdf

Kunkle, F., & Helderman, R. S. (2010, February 10). Human microchips seen by some in Virginia House as device of antichrist. An issue of privacy or sign of the apocalypse? *The Washington Post*. Retrieved from http://articles.washingtonpost.com/2010-02-10/news/36905186_1_microchips-privacy-issues-beast

Lawson, S. (2008, October 24). Researchers find Problems with RFID Passport Cards. *PC World Business Centre*. Retrieved from http://www.goodgearguide.com.au/article/264964/researchers_find_problems_rfid_passport_cards/

Lehman, S. (2012, March 22). *Brazilian City Uses Computer Chips Embedded in School Uniforms to Keep Track of Students*. The Associated Press. Retrieved from http://www.newser.com/article/d9tlnip00/brazilian-city-uses-computer-chips-embedded-in-school-uniforms-to-keep-track-of-students.html

Lewan, T. (2009, July 12). Special alloy sleeves urged to block hackers? *Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2009/07/11/AR2009071101929_pf.html

Lewan, T. (2009, July 11). *Chips in official IDs raise privacy fears*. Phys.org. Retrieved from http://phys.org/news166552331.html

Liao, D. & Edelson, S. D. (2010). *U.S. Patent No. 7,784,693*. Washington, DC: U.S. Patent and Trademark Office.

Lim, T.L. & Li, T. (2008, March 31). Flexible Privacy Protection for RFID Tags via Selective Identifier Masking. *Proceedings of the IEEE Wireless Communications and Networking Conference*, pp. 1570-1575. Retrieved from http://ieeexplore.ieee.org/iel5/4489030/4489031/04489312.pdf

Lindley, S. E. (2013). *U.S. Patent No. D690,767*. Washington, DC: U.S. Patent and Trademark Office.

Lowe, P. R. (2009). *U.S. Patent No. 7,523,870*. Washington, DC: U.S. Patent and Trademark Office.

Mahmood, R. A., & Al-Hamdani, W.A. (2011, October 7). Is RFID Technology Secure and Private? *Proceedings of the 2011 Information Security Curriculum Development Conference*, pp. 42-49. Retrieved from http://dl.acm.org/citation.cfm?id=2047462

Maniyan, A., Ghassemi, R. A., & Rahrovy, E. (2012). A survey of the Role and the Applications of Radio Frequency Identification (RFID) Technology in the Efficiency of Supply Chain Management (SCM) with an emphasis on Food Industries. *International Journal of Learning & Development. vol. 2, no. 5*. Retrieved from http://www.macrothink.org/journal/index.php/ijld/article/viewFile/2299/2020

Marquardt, N., Taylor, A.S., Villar, N., & Greenberg, S. (2010, April 10). Rethinking RFID: Awareness and Control for Interaction with RFID Systems. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 2307-2316. Retrieved from http://dl.acm.org/citation.cfm?id=1753674

Marquardt, N., Taylor, A.S., Villar, N., & Greenberg, S. (2010, April 10). Visible and Controllable RFID Tags. *Proceedings of CHI EA '10 CHI '10 Extended Abstracts on Human Factors in Computing Systems*, pp. 3057-3062. Retrieved from http://dl.acm.org/citation.cfm?id=1753917

Masuta, T. (2008). U.S. *Patent No. 7,387,233*. Washington, DC: U.S. Patent and Trademark Office.

Maus, C. T. (2011). U.S. *Patent No. 8,066,192*. Washington, DC: U.S. Patent and Trademark Office.

Maus, C. T. (2014). U.S. *Patent No. 8,800,877*. Washington, DC: U.S. Patent and Trademark Office.

McNamara, P. (2009, April 8). Mich. lawmaker urges governor to rethink RFID in licenses. *Network World*. Retrieved from http://www.networkworld.com/community/node/40717

Metras, H. (2005, October 12). RFID Tags for Ambient Intelligence: Present Solutions and Future Challenges. *Proceedings of the 2005 joint conference on Smart objects and ambient intelligence: innovative context-aware services: usages and technologies*, pp 43-46. Retrieved from http://dl.acm.org/citation.cfm?id=1107565

Narendra, S. G., Tadepalli, P., & Chakraborty, S. (2011). *U.S. Patent No. 7,961,101*. Washington, DC: U.S. Patent and Trademark Office.

Nogueira, M. & Greis, N. (December, 2009). *Uses of RFID Technology in U.S. Identification Documents* [Research brief]. Retrieved from http://www.kenan-flagler.unc.edu/~/media/Files/kenaninstitute/CLDS/IHSSResearchBrief_RFID.pdf

O'Byrne, H. D., Smith, S. W., & Pauley, J. D. (2011). *U.S Patent No. 7,932,813*. Washington, DC: U.S. Patent and Trademark Office.

Ohkawa, T., Yuyama, M., Yoshigi, H., Oonishi, T., & Watanabe, K. (2005). *U.S. Patent No. 6,972,662*. Washington, DC: U.S. Patent and Trademark Office.

Periaswamy, S. C. G., Thompson, D. R., & Di, J. (2011). Fingerprinting RFID Tags. *IEEE Transactions on Dependable and Secure Computing. vol. 8, no. 6*. Retrieved from http://comp.uark.edu/~drt/pubs/2011/Fingerprinting_RFID_Tags2011copyright.pdf

Philips Semiconductors. (2002). *mifare® (14443A) 13.56 MHz RFID Proximity Antennas* [Data file]. Public Revision 1.0. Retrieved from http://www.nxp.com/documents/application_note/AN78010.pdf

Phillips, T., Karygiannis, T., & Kuhn, R. (2005, December 12). Security Standards for the RFID Market. *IEEE Security & Privacy*. Retrieved from http://ieeexplore.ieee.org/iel5/8013/33104/01556544.pdf

Qaiser, A., & Khan, S. (2006, November 13). Automation of Time and Attendance using RFID Systems. *Proceedings of the 2nd International Conference on Emerging Technologies*, pp.60-63. Retrieved from http://ieeexplore.ieee.org/iel5/4136870/4117909/04136896.pdf

Qiao, Y., Chen, S., & Li, T. (2013). RFID as an Infrastructure. *Springer Briefs in Computer Science*. Retrieved from https://www.springer.com/engineering/electronics/book/978-1-4614-5229-4

Ramos, A., Scott, W., Lloyd, D., O'Leary, K., & Waldo, J. (2009, October 1). A Threat Analysis of RFID Passports. *Communications of the ACM, vol. 52, no. 12*, pp. 38-42. Retrieved from http://queue.acm.org/detail.cfm?id=1626175

Rau, C. C., & Hsaio, C. S. (2012, August 24). Constructing a Security-Mechanism RFID System. *Proceedings of the 2012 International Conference on Anti-Counterfeiting, Security, and Identification*, pp. 1-3. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6325288

RFID Glossary. (n.d.). Alliance Group Document & Records Management. Retrieved April 3, 2014, from http://www.alliancegroup.co.uk/rfid-glossary.htm

Rieback, M. R., Gaydadjiev, G. N., Crispo, B., Hofman, R. F. H., & Tanenbaum, A. S. (2006, December 3). A Platform for RFID Security and Privacy Administration. *20th Large Installation System Administration Conference*. Retrieved from http://www.usenix.org/event/lisa06/tech/rieback/rieback.pdf

Roberti, M. (2009, August 10). Are RFID's Benefits to Apparel Retailers Real or Hype? *RFID Journal*. Retrieved from http://www.rfidjournal.com/articles/view?5112

Schneier, B. (2008, January 21). Information is our only security weapon. (S. Stokely, Ed.). *Keynote address at Linux Australia Conference*. Retrieved from http://www.schneier.com/news-051.html

Selker, E. J. (2005). *U.S. Patent No. 6,863,220*. Washington, DC: U.S. Patent and Trademark Office.

Shahzad, M. & Liu, A. X. (2012, August 22). Every Bit Counts - Fast and Scalable RFID Estimation. *Proceedings of ACM MobiCom'12 Conference*, pp. 365-376. Retrieved from https://www.cse.msu.edu/~alexliu/publications/RFIDEstimation/RFIDEstimationMobicom.pdf

Shaughnessy, M. (2010, March 3). Labeling the Consumer: how mindless ID-scanning can hurt customers. *BoingBoing*. Retrieved from http://boingboing.net/2010/03/03/labeling-the-consume.html

Shimizu, M., Takenaka, H., & Tanaka, S. (2000). *U.S. Patent No. 6,097,622*. Washington, DC: U.S. Patent and Trademark Office.

Smith, M. (2010, July 27). The Next Big Privacy Concern: RFID "Spychips". *Network World*. Retrieved from http://www.networkworld.com/community/blog/next-big-privacy-concern-rfid-%E2%80%9Cspychips%E2%80%9D

Smith, S.W. & Spafford, E.H. (2004, February 19). Grand Challenges in Information Security: Process and Output. *IEEE Security & Privacy, 2(1)*. Retrieved from https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/01264859.pdf

Stoltz, M. (2014, June). *Electronic driver's licenses: Driving towards the future*. Whitepaper for NXP Semiconductors. Retrieved from http://www.nxp.com/documents/white_paper/75017570.pdf

Suzuki, H. (2008). *U.S. Patent No. 7,439,781*. Washington, DC: U.S. Patent and Trademark Office.

Swedberg, C. (2012, October 11). Murata Mass-Produces 'World's Smallest HF Tag'. *RFID Journal*. Retrieved from http://www.rfidjournal.com/articles/view?10017

Sweeney, W. R. (2014). *U.S. Patent No. 8,624,740*. Washington, DC: U.S. Patent and Trademark Office.

Tanner, C. (2010). *U.S. Patent No. 7,762,471*. Washington, DC: U.S. Patent and Trademark Office.

Timmer, J. (2008, October 2). RFID passport hack has scanner seeing visions of Elvis. *Ars Technica*. Retrieved from http://arstechnica.com/security/2008/10/rfid-passport-hack-has-scanners-seeing-visions-of-elvis/

United States Census Bureau. (2013). [National population statistics]. Retrieved from http://quickfacts.census.gov/qfd/states/00000.html

U.S. Customs and Border Protecton. (2014, March 26). *Info Center*. What is an Enhanced Driver's License (EDL). Retrieved from https://help.cbp.gov/app/answers/detail/a_id/1269/

Want, R. (2004, October 1). The Magic of RFID. *ACM Queue, vol. 2, no. 7*. Retrieved from http://queue.acm.org/detail.cfm?id=1035619

Washington State Department of Licensing. (2015). *Frequently asked questions: EDL/EID.* Retrieved from http://www.dol.wa.gov/driverslicense/edlfaq.html

Williams, I. (2009, April 15). *South Africa rolls out biometric passports*. Incisive Media. Retrieved from http://www.v3.co.uk/v3-uk/news/2001299/south-africa-rolls-biometric-passports

Xiang-jie, N. & Hua, L. (2014, March 10). Lower Power Design for UHF RF CMOS Circuits Based on the Power Consumption Acuity. *Mathematical Problems in Engineering*. Retrieved from http://dx.doi.org/10.1155/2014/512398

Yuengling, J. (2009). *U.S. Patent No. D597,307*. Washington, DC: U.S. Patent and Trademark Office.

Yuengling, J. (2011). *U.S. Patent No. D635,359*. Washington, DC: U.S. Patent and Trademark Office.

Zuili, P. J. (2013). *U.S. Patent No. 8,397,988*. Washington, DC: U.S. Patent and Trademark Office.

APPENDIX

APPENDIX

These are details of the search through existing Patent applications for prior work similar to that proposed for this dissertation.

The text and illustrations were read for every patent since 1976 the title of which contained the terms "RFID" and "card". A total of 35 patents were reviewed:

Secure data card with passive RFID chip and biometric sensor
(U.S. Patent No. 8,823,497, 2014)

Security feature RFID card
(U.S. Patent No. 8,820,639, 2014)

Dynamic information radio-frequency identification (RFID) card with biometric capabilities
(U.S. Patent No. 8,816,819, 2014)

RFID reporting personal health card and related systems
(U.S. Patent No. 8,800,877, 2014)

Turbo card table game with RFID card identifier
(U.S. Patent No. 8,777,727, 2014)

Switchable RFID card reader antenna
(U.S. Patent No. 8,763,893, 2014)

Semi-rigid radio frequency identification (RFID) card, manufacturing method and machine for its production
(U.S. Patent No. 8,746,575, 2014)

Controllable RFID card
(U.S. Patent No. 8,624,740, 2014)

RFID clamshell style card
(U.S. Patent No. D690, 767, 2013)

Method and system for securing a transaction using a card generator, a RFID generator, and a challenge response protocol
(U.S. Patent No. 8,397,988, 2013)

Integrated RFID tag in a card holder, cage, lid, and rack for use with inventorying and tracking of cage occupants and equipment
(U.S. Patent No. 8,161,910, 2012)

Light enabled RFID card
(U.S. Patent No. 8,111,160, 2012)

RFID reporting personal health card and related systems
(U.S. Patent No. 8,066,192, 2011)

Small RFID card with integrated inductive element
(U.S. Patent No. 7,961,101, 2011)

Sampling to obtain signal from RFID card
(U.S Patent No. 7,932,813, 2011)

Silicone card frame with RFID payment device
(U.S. Patent No. D635, 359, 2011)

Circuit arrangement for wirelessly exchanging data and RFID chip card device
(U.S. Patent No. 7,912,430, 2011)

RFID card using Korea paper and the manufacturing method thereof
(U.S. Patent No. 7,909,258, 2011)

Semiconductor device, IC card, IC tag, RFID, transponder, paper money, valuable securities, passport, electronic device, bag, and clothes
(U.S. Patent No. 7,795,617, 2010)

Assembly of SIM card and RFID antenna
(U.S. Patent No. 7,784,693, 2010)

Proximity payment card with cost-effective connection between user-actuatable input switch and RFID IC
(U.S. Patent No. 7,762,471, 2010)

Manufacturing method of semiconductor device, and IC card, IC tag, RFID, transponder, bill, securities, passport, electronic apparatus, bag, and garment
(U.S. Patent No. 7,666,722, 2010)

Semiconductor device, IC card, IC tag, RFID, transponder, bills, securities, passport, electronic apparatus, bag, and clothes
(U.S. Patent No. 7,663,473, 2010)

Currency dispensing ATM with RFID card reader
(U.S. Patent No. 7,584,885, 2009)

Silicone card frame clip with RFID payment device
(U.S. Patent No. D597, 307, 2009)

Memory module and card with integrated RFID tag
(U.S. Patent No. 7,564,359, 2009)

RFID card retention assembly
(U.S. Patent No. 7,523,870, 2009)

Power detection circuit for non-contact IC card or RFID tag
(U.S. Patent No. 7,439,781, 2008)

RFID card issuing system
(U.S. Patent No. 7,387,233, 2008)

Mobile terminal having smart card coupled with RFID tag and method for performing RFID function in such mobile terminal
(U.S. Patent No. 7,374,100, 2008)

ATM with RFID card, note, and check reading capabilities
(U.S. Patent No. 7,284,692, 2007)

Currency dispensing ATM with RFID card reader
(U.S. Patent No. 7,004,385, 2006)

RFID (radio frequency identification) and IC card
(U.S. Patent No. 6,972,662, 2005)

Manually operated switch for enabling and disabling an RFID card
(U.S. Patent No. 6,863,220, 2005)

Ferroelectric memory used for the RFID system, method for driving the same, semiconductor chip and ID card
(U.S. Patent No. 6,097,622, 2000)

None of these patents incorporate the multiple-region card nor the selective detuning method described in this dissertation. The nearest in concept were 8,624,740 (2014); 7,762,471 (2010); and 6,863,220 (2005); which involved switchable functions, but no antenna overlay. Of these, the closest prior work was probably 6,863,220, as it does mention capacitive coupling. What sets it apart, though, is that it calls for an external key device to enable data transfer, rather than the conductive overlay to disable it (2005).

Patents were also searched with the additional strings "select", "cover", "overlay", "field", and "privacy" (individually appended). No matching patents were found. With "security", one patent was found:

Security feature RFID card
(U.S. Patent No. 8,820,639, 2014)
It deals primarily with optical scanning, and makes no mention of field selection (2014).

With "data", two more were found:

Secure data card with passive RFID chip and biometric sensor
(U.S. Patent No. 8,823,497, 2014)
This deals with biometrics rather than RF selection (2014).

Circuit arrangement for wirelessly exchanging data and RFID chip card device
(U.S. Patent No. 7,912,430, 2011)
This deals with security only in terms of encryption, and is unrelated to hardware overlays (2011).

VITA

VITA

Robert Winkworth graduated Summa Cum Laude with his Bachelor of Science in Information Technology, and again with his Master of Science in Information Systems, culminating in thesis work on enterprise networking in Linux-based operating systems. Both the mobile wireless hardware and data routing software were of his own design and development. At the head of his class, he amassed enough advance placement credits to complete his first graduate degree in under a year, with multiple distinctions and several labs established under his leadership. He holds over a dozen professional certifications from his work as a network technician, systems analyst, wireless engineer, and laboratory specialist. His principle research interests at Purdue have focused on forensic technology, embedded systems, and wireless communication standards. He lives with his partner on the Pacific coast, consulting for Fortune 500 companies and exceptional entrepreneurs. He also teaches youth workshops in various technological topics.