

New Directions in Advanced RFID Systems

DISSERTATION SUBMITTED TO
THE SCHOOL OF ELECTRICAL AND ELECTRONIC ENGINEERING
OF THE UNIVERSITY OF ADELAIDE

BY

Damith Chinthana Ranasinghe

IN FULFILMENT OF THE REQUIREMENTS FOR THE
DEGREE OF DOCTOR OF PHILOSOPHY

January 2007

Abstract

A combination of Radio Frequency Identification technology and ubiquitous computing are revolutionising the manner in which we look at simple objects. Radio Frequency Identification (RFID) allows RFID labeled objects to be identified at a distance without physical contact, and ubiquitous computing provides a virtually connected environment for the objects. RFID labels are frequently referred to as the next generation barcodes.

RFID Systems provide increased productivity, efficiency, convenience and many advantages over bar codes for numerous applications, especially global supply chain management.

RFID labeling has a number of advantages over conventional bar code systems. The optics based bar code systems could be rendered useless by common everyday environments containing dirt, dust, smoke, grease, condensation and by misorientation and misalignment. Furthermore bar codes are subject to fraudulent duplication and counterfeiting with minimal effort.

However, there are limitations and constraints inherent to RFID technology: semiconductor thresholds, limits on transmitted power, costs, antenna and coupling inefficiencies. Thus it is important for RFID designers to understand these limitations and constraints in order to optimise system designs and overcome inefficiencies where possible. Therefore the work presented in this dissertation seeks to improve the performance of advanced RFID systems by overcoming a number of these limitations.

Prior to a discussion of improving performance, the author's interpretation of a modern RFID system along its evolutionary path as a ubiquitous RFID network and its application to supply chain management is described. Performance improvements are achieved by: the development of electromagnetic theory for RFID system analysis and optimisation; design and development of interrogator antennas; analysis of electrically small and tiny antennas for RFID labels; and development and utilisation of a design methodology for creating high performance label antennas and antennas for tagging metallic objects.

Implementations of RFID systems have raised concerns regarding information security and possible violations of end-user privacy. The most profound concerns are raised against low cost RFID technology because of its potential for mass scale deployment, its pervasive nature, and the resource limitations preventing the provision of strong cryptographic solutions. There is a growing need in the RFID community to discover and develop techniques and methods to overcome various hurdles posed by the above-mentioned concerns.

Thus, the thesis also considers the vulnerabilities of low cost RFID systems and associated insecurities and privacy concerns resulting from the latter. Prior to addressing such concerns impeding the deployment of low cost RFID technology, a framework within

which to provide security services is also detailed. It has become important to both define and identify a framework based around low cost RFID systems since RFID has become a “catch all” phrase for various other forms of technology.

Addressing security and privacy of low cost RFID systems requires novel thinking. The later parts of the thesis outline design considerations for security mechanisms and a number of practicable solutions for providing the features of: mutual authentication; confidentiality; message content security; product authentication; anonymity and untraceability, that are necessary for low cost RFID systems to overcome the weaknesses identified in this dissertation. Implementing these security mechanisms requires the generation of true random tag parameters and true random numbers. Achieving these objectives using a hardware based true random number generator is also described and analysed.

A final part of the thesis focuses on active RFID labels and improving their performance. The primary concern with active labels is the life of the onboard battery. Turn-on circuits provide a method of turning “on” and “off” an active label remotely to conserve valuable battery power. Analysis, development and testing of a turn-on circuit concept, based on interrogator field sensing, have provided a means of remotely activating and deactivating active RFID labels and conserving battery power. The final chapter of this thesis provides a detailed analysis, based on coupling relations between electromechanical systems, for evaluating the feasibility of a theft detection sensor, based on a turn-on circuit for an active RFID label, for preventing the theft of high value items.

While low cost RFID needs to overcome certain security and privacy related barriers, RFID technology does provide novel and valid approaches to such security related applications as product authentication, anti-counterfeiting and theft detection. It is believed that the contributions from this thesis will extend and elaborate on the existing knowledge base, paving the way forward to allow further significant deployment of advanced RFID technology.

CONTENTS

Chapter 1	29
INTRODUCTION	29
1.1 Overview.....	30
1.2 Problem Statements	31
1.3 Thesis Contributions	33
1.4 Thesis Organisation	34
1.4.1 Part One: Electromagnetic Coupling.....	35
1.4.2 Part Two: Vulnerabilities and Solutions.....	36
1.4.3 Part Three: Turn-on Circuits.....	36
1.5 Publications.....	37
1.6 Notational Aspects.....	39
 Chapter 2	 43
NETWORKED RFID SYSTEMS	43
2.1 RFID Systems Overview.....	44
2.2 RFID Labels.....	45
2.2.1 Label to Interrogator Communication.....	47
2.2.2 EPC Concept	48
2.2.3 Label Hierarchies.....	49
2.2.3.1 A Classless RFID Label Society	50
2.3 Interrogators.....	50
2.4 Back-End Systems.....	51
2.5 Anti-Collision.....	51
2.6 Conclusion	54

Chapter 3	57
EPC NETWORK ARCHITECTURE.....	57
3.1 Introduction.....	58
3.1.1 N-tier Service Oriented Architecture.....	58
3.2 EPC Network	59
3.3 RFID Components.....	62
3.4 Application Level Event (ALE) Engine.....	62
3.4.1 EPC Data Encapsulation and Reporting.....	63
3.5 Object Name Service	64
3.6 EPC Information Service	67
3.7 An EPC Network Application	68
3.8 Supply Chain Management	69
3.9 Solutions to Grey-Market Activity and Counterfeiting	70
3.10 Product Recall and Other improvements.....	71
3.11 Conclusion	72
 Chapter 4	 73
ELECTROMAGNETICS AND COUPLING	73
4.1 Electromagnetic Fields.....	74
4.2 Fundamental Laws of Electromagnetics.....	74
4.2.1 Faraday's Law	74
4.2.2 Ampere's Law as Modified by Maxwell.....	74
4.2.3 Gauss' Law for Electric Flux	75
4.2.4 Gauss' Law for Magnetic Flux.....	75
4.2.5 Concept of a Source and a Vortex.....	75
4.3 Boundary Conditions	76
4.4 Electromagnetic Waves.....	77
4.5 Retarded Potentials	79
4.6 Radiation.....	79
4.7 Electric Dipole.....	80
4.8 Magnetic Dipole	80
4.9 Transmitting Antenna Concepts	81

4.10	Characteristics of Near and Far Fields	81
4.11	Near and Far Field Measures.....	82
4.12	Reciprocity.....	82
4.13	RFID Label Antenna and Reader Antenna Coupling.....	83
4.13.1	Near Field Coupling - Magnetic Field.....	84
4.13.2	Near Field Coupling - Electric Field	84
4.13.3	Far Field Coupling	84
4.14	Development of Coupling Volume Theory	86
4.14.1	Near Field – Magnetic Field.....	86
4.14.1.1	Coupling Volume of a Magnetic Loop	87
4.14.1.2	Coupling Volume of a Solenoid.....	87
4.14.2	Near Field – Electric Field.....	87
4.14.2.1	Coupling Volume of a General Shape	88
4.14.2.2	Coupling Volume of a Rectangular Capacitor.....	89
4.14.3	Far Field Coupling Volume Theory	90
4.15	A Relation Between Electrostatic and Electrodynamic Theory	91
4.16	Conclusion	91

Chapter 5 **93**

	NEAR FIELD INTERROGATOR ANTENNA DESIGN.....	93
5.1	Electromagnetic Compatibility Constraints.....	94
5.2	Near Field Creation Interrogator Antennas.....	95
5.3	Interrogator Antenna Equivalent Circuits.....	97
5.4	Wedge Above a Ground Plane Antenna.....	98
5.5	A Relation between Electrostatic and Electrodynamic Theory.....	102
5.6	Large Loop Antennas.....	104
5.6.1	Practical Construction of a Large Loop Antenna	106
5.6.2	Large Loop Antenna Model.....	112
5.7	Experimental results	114
5.8	Interrogation at a Large Distance.....	115
5.9	Conclusion	116

Chapter 6	119
FAR FIELD RFID LABEL ANTENNA DESIGN	119
6.1 RFID Label Antennas	120
6.1.1 Magnetic Field Sensitive Antennas.....	120
6.1.2 Electric Field Sensitive Antennas	122
6.1.3 Electromagnetic Field Antennas	122
6.2 Label Antenna Design Considerations	123
6.2.1 Nature of Antennas for RFID	124
6.2.2 Label Antenna Equivalent Circuits	126
6.2.3 Matching to an RFID Chip Impedance.....	127
6.2.4 Environmental Constraints	130
6.2.5 Performance Measure.....	131
6.3 Label Antenna Design.....	133
6.3.1 Design Requirements	133
6.3.2 Design Methodology.....	134
6.4 Illustrating a Novel Antenna Design.....	136
6.4.1 Antenna Requirements, Material and RFID IC Impedance	136
6.4.2 Antenna Type	137
6.4.3 Bow Tie Antenna Design	141
6.4.4 Bow Tie Antenna with a Parallel Tuning Inductor.....	142
6.4.5 Bow Tie Antenna with a Series Tuning Inductor	146
6.5 Conclusion	154
 Chapter 7	 155
SMALL FAR FIELD RFID LABEL ANTENNAS	155
7.1 Introduction.....	156
7.2 Radiation Quality Factor	156
7.2.1 Bandwidth	159
7.2.2 Matching	161
7.3 Antenna Quality Factor.....	161
7.3.1 Bandwidth	162
7.3.2 Efficiency	162

7.4	Difficulty: Narrow Bandwidth Antennas and Impedance Matching	163
7.5	A Novel Electrically Small Antenna for Tagging Metallic Objects	164
7.5.1	Antenna Requirements, Materials and RFID IC Impedance.....	165
7.5.2	Antenna Design	166
7.5.3	Simulation	167
7.5.4	Measured Results.....	168
7.5.5	Performance	172
7.6	Conclusion	173

Chapter 8 **175**

TINY ANTENNAS AND FAR FIELD COUPLING VOLUME THEORY	175
8.1 Far Field Coupling Volume Theory.....	176
8.1.1 Analysis of a Tiny Loop.....	176
8.2 Application to Antenna Comparison.....	178
8.2.1 Loop Antenna Structure	179
8.2.2 Bow Tie Antenna Structure	180
8.2.3 Comparison	181
8.3 Application to Power Transfer Analysis	181
8.3.1 Miniature antenna properties	182
8.3.2 Reactive Power Density per Unit Volume.....	183
8.3.3 Label Coupling Volume	183
8.3.4 Reactive Power in Short Circuit Label.....	184
8.3.5 Power Delivered to a Tuned Label.....	184
8.3.6 Reactive Power in Tuned Coil.....	184
8.3.7 Reactive Power Needed in the Depletion Layer Capacitance	185
8.3.8 Analysis Results.....	185
8.4 Conclusion	188

Chapter 9 **191**

SECURITY AND PRIVACY	191
9.1 Introduction.....	192

9.2	Characteristics of a Low Cost RFID System	192
9.2.1	A Low Cost Tag	192
9.2.1.1	RF Front-end.....	193
9.2.1.2	Memory Circuitry.....	193
9.2.1.3	Finite State Machine (Logic Circuitry).....	194
9.2.2	Tag Cost	194
9.2.2.1	Manufacturing Costs	195
9.2.3	Tag Power Consumption	195
9.2.4	Physical Protection (Tamper Proofing)	196
9.2.5	Standards.....	196
9.2.6	System Operational Requirements	196
9.2.7	Communication Range.....	197
9.2.8	Frequency of Operation and Regulations	197
9.2.9	Security Provided by Class I and Class II labels	198
9.2.9.1	Security Features of Class I Generation 2 Labels	199
9.2.9.2	Security Features Expected from Class II Labels	199
9.2.9.3	Backend System Services: Track and Trace Capability	200
9.3	Vulnerabilities of Low Cost RFID Systems	200
9.3.1	Eavesdropping and Scanning.....	200
9.3.1.1	Passive Eavesdropping	202
9.3.1.2	Scanning (Active eavesdropping).....	203
9.3.2	Cloning.....	203
9.3.3	Man-in-the-Middle.....	204
9.3.4	Denial of Service	204
9.3.4.1	Code Injection.....	204
9.3.5	Communication Layer Weaknesses	205
9.3.6	Physical Attacks.....	206
9.3.6.1	Non-Invasive Attacks	206
9.3.6.2	Invasive Attacks.....	207
9.3.7	Privacy Violations.....	207

9.3.7.1	Profiling.....	207
9.3.7.2	Tracking and Surveillance	208
9.4	Addressing Vulnerabilities	208
9.5	Addressing Security Issues.....	210
9.5.1	Confidentiality.....	210
9.5.2	Message Content Security	211
9.5.3	Authentication	211
9.5.3.1	Tag and Interrogator Authentication.....	211
9.5.3.2	Product Authentication	211
9.5.4	Access Control.....	212
9.5.5	Availability.....	212
9.5.6	Integrity.....	212
9.6	Addressing Violations of Privacy	212
9.6.1	Anonymity.....	214
9.6.2	Untraceability (Location Privacy).....	214
9.7	Cryptography.....	215
9.7.1	Cryptographic primitives.....	215
9.7.2	Classification of Attacks.....	217
9.7.2.1	Attacks on Cryptographic Primitives	217
9.7.2.2	Attacks on Protocols.....	218
9.7.3	Level of Security.....	218
9.8	Low Cost RFID and Cryptography.....	220
9.8.1	Challenges	220
9.9	A Survey of Solutions.....	223
9.9.1	Cryptographic Hash Functions	223
9.9.2	Cellular Automata.....	225
9.9.3	Linear and Non Linear Feedback Shift Registers.....	225
9.9.4	Message Authentication Codes.....	225
9.9.5	NTRU	226
9.9.6	Tiny Encryption Algorithm	226
9.9.7	Scalable Encryption Algorithm.....	227

9.9.8	Re-encryption	227
9.9.9	Lightweight Cryptography	228
9.9.9.1	Lightweight Hardware.....	228
9.9.9.2	Lightweight Protocols.....	229
9.9.10	Minimalist Cryptography	229
9.9.10.1	Pseudonyms	229
9.9.10.2	One Time Pads and Random Numbers	230
9.9.11	Exploiting Noise	231
9.9.12	Radio Fingerprinting	231
9.9.13	Distance Implied Distrust	231
9.9.14	Authentication Protocols	232
9.10	Conclusion	232

Chapter 10 **235**

EVALUATION FRAMEWORK.....	235
10.1 Evaluation Framework.....	236
10.2 Evaluating Security Measures	236
10.3 Evaluating Cost and Performance Objectives.....	237
10.3.1 Tag Implementation Cost	237
10.3.2 Backend Resources and Overhead Costs.....	238
10.3.3 Power Consumption.....	239
10.3.4 Performance	239
10.4 Security Model	240
10.4.1 Authorised and Legitimate	240
10.4.2 Tamper Proofing.....	240
10.4.3 System Model.....	241
10.4.4 Adversary Model	243
10.4.5 Objectives of an Adversary	243
10.4.6 Level of Interference.....	243
10.4.7 Presence	244
10.4.8 Available Resources.....	244

10.5 Conclusion	245
Chapter 11	247
SECURITY AND PRIVACY BASED ON LIGHTWEIGHT CRYPTOGRAPHY	247
11.1 Introduction.....	248
11.1.1 Notation.....	248
11.2 Related Work	249
11.2.1 XOR Operation.....	249
11.2.2 CRC Generation	249
11.2.3 Stream Ciphers	250
11.2.3.1 Linear Feed Back Shift Registers	252
11.2.3.2 Implementation Considerations.....	253
11.2.3.3 Nonlinear Filter Generators.....	254
11.2.3.4 Clock Controlled Generator.....	255
11.2.3.5 Power Consumption	257
11.2.4 Physically Uncloneable Functions	259
11.2.4.1 Circuit Implementation.....	261
11.3 Authentication	262
11.3.1.1 Challenge-and-Response Protocols	263
11.3.1.2 Constructing a Challenge-and-Response Protocol.....	263
11.3.1.3 Tag Authentication.....	264
11.3.1.4 Tag and Reader Authentication (Mutual Authentication).....	266
11.3.1.5 Hash Based Tag Authentication.....	267
11.3.1.6 Evaluation.....	268
11.3.1.7 Removing Barriers to Performance	269
11.3.1.8 Evaluating the Improved Performance	269
11.3.1.9 Addressing Reliability Issues	271
11.3.1.10 Practical Issues.....	273
11.3.1.11 Possible Attacks	274
11.3.1.12 Conclusion.....	274

11.4 Confidentiality and Authentication.....	275
11.4.1 Secure Forward Link.....	275
11.4.2 Tag and Reader Authentication (Mutual Authentication).....	276
11.4.3 Evaluation.....	277
11.4.4 Practical Issues.....	279
11.4.5 Possible Attacks.....	279
11.4.6 Conclusions.....	279
11.5 Anonymity and Untraceability.....	280
11.5.1 Pseudonyms.....	280
11.5.2 Re-encryption.....	280
11.5.2.1 Evaluation.....	283
11.5.2.2 Practical Issues.....	285
11.5.2.3 Possible Attacks.....	286
11.5.3 Randomly Varying Object Identifiers.....	288
11.5.3.1 Evaluation.....	289
11.5.3.2 Practical Issues.....	290
11.5.3.3 Possible Attacks.....	292
11.6 Anonymity, Untraceability, and Product Authentication.....	292
11.6.1 Product Authentication.....	293
11.6.1.1 Evaluation.....	295
11.6.1.2 Practical Issues.....	297
11.6.1.3 Possible Attacks.....	297
11.7 Acknowledgements.....	297
11.8 Conclusion.....	298

Chapter 12 **301**

HARDWARE BASED RANDOM NUMBER GENERATOR.....	301
12.1 Introduction.....	302
12.2 Sources of Randomness.....	303
12.3 Metastability.....	304
12.4 Random Number Generator Design.....	305

12.4.1	Circuit Implementation	305
12.4.2	Design Analysis	306
12.4.3	Increasing the Dynamic Range of Operation	307
12.5	Evaluation of the Generator.....	308
12.5.1	Chaos Theory (Dynamic System Analysis).....	308
12.5.1.1	Attractors	309
12.5.1.2	Phase Space Reconstruction.....	309
12.5.2	Statistical Testing.....	310
12.5.2.1	Hypothesis Testing.....	310
12.5.2.2	Statistical Test Suite	311
12.6	Analysis and Interpretation of the Test Results	312
12.6.1	Post Processing	312
12.6.2	System Analysis.....	313
12.6.3	Statistical Testing.....	316
12.6.3.1	Parameters Used in the Test Suite	316
12.6.3.2	Evaluation of Test Results	316
12.6.3.3	Proportion of Sequences Passing a Test.....	318
12.6.3.4	Uniform Distribution of P -values.....	319
12.7	Acknowledgements.....	320
12.8	Conclusion	321

Chapter 13 **325**

TURN-ON CIRCUITS FOR ACTIVE LABELS.....	325	
13.1	Introduction.....	326
13.2	Turn on circuits	326
13.2.1	Evaluating Turn-On Circuit Concepts.....	327
13.2.2	Turn on Range Estimation for a Zero Power Turn on Circuit	333
13.2.3	Turn on Range Estimation for a Low-Power Turn on Circuit.....	335
13.3	Design and Implementation.....	336
13.3.1	Zero Power Turn-On Circuit	337
13.3.2	Low Power Turn-On Circuit.....	340

13.4 Acknowledgements.....	340
13.5 Conclusions.....	340

Chapter 14 **343**

AN APPLICATION OF A MEMS BASED TURN-ON CIRCUIT 343

14.1 Introduction.....	344
14.2 Theft Detection Circuit	344
14.3 Magnetic-Electroacoustic Energy Conversion System.....	345
14.4 Analysis	348
14.4.1 Electroacoustic Energy Conversion	348
14.4.2 Electrical Power.....	349
14.4.3 Mechanical Power.....	351
14.4.4 Mechanical Resonance.....	352
14.4.5 Zero Power Turn-On Requirements.....	353
14.5 Practical Evaluation.....	353
14.6 Acknowledgements.....	358
14.7 Conclusions.....	358

Appendix A **361**

LIST OF FORMULAE AND SPICE MODEL..... 361

A.1 Inductance Calculations	361
A.2 Axial Field of a Circular Coil.....	362
A.3 Skin Effect	362
A.4 Radiation Resistances	362
A.5 SBD SPICE Model.....	363