



Ultralightweight Cryptography for Low Cost Passive RFID Tags

Submitted by

Umar Mujahid Khokhar

Supervised by

Prof. Dr. M. Najam-ul-Islam

In Partial fulfilment of the degree of
Doctor of Philosophy in Electrical Engineering

Bahria University, Islamabad

June, 2016

Certificate of Originality

This is to certify that the intellectual contents of the thesis

Ultralightweight Cryptography for Low Cost Passive RFID Tags

are the product of my own research work except, as cited properly and accurately in the acknowledgements and references, the material taken from such sources as research papers, research journals, books, internet, etc. solely to support, elaborate, compare and extend the earlier work. Further, this work has not been submitted by me previously for any degree, nor it shall be submitted by me in the future for obtaining any degree from this University, or any other university or institution. The incorrectness of this information, if proved at any stage, shall authorize the university to cancel my degree.

Signature: _____

Date: _____

Name of the Research Candidate: Umar Mujahid Khokhar

**Certificate of Completion
of
Thesis Work**

This is to certify that

Mr. Umar Mujahid Khokhar

has successfully completed his research thesis, titled

“Ultralightweight Cryptography for Low cost Passive RFID Tags”

under my supervision. The thesis meets the scholarly standards as set

by Bahria University, Pakistan

Date: _____

Research Supervisor (Signature)

Name: Prof. Dr. M. Najam-ul-Islam

Affiliation: Bahria University, Islamabad

List of Publications

Journals

1. Umar Mujahid, M. Najam-ul-Islam, and M. Ali Shami, "RCIA: A New Ultralightweight RFID Authentication Protocol Using Recursive Hash", International Journal of Distributed Sensor Networks, Vol. 2015, Article ID 642180, 2015. doi:10.1155/2015/642180. (IF-0.663)
2. Umar Mujahid, Atif Raza Jafri, M. Najam-ul-Islam, "Efficient Hardware Implementation of Ultralightweight RFID Mutual Authentication Protocol", Journal of Circuit, System and Computers Vol. 25, No. 7 (2016) Article ID, 1650078 (19 pages) (IF-0.25)
3. Umar Mujahid, M. Najam-ul-Islam, Atif Raza Jafri, Qurat-ul-Ain and M. Ali Shami, "A New Ultralightweight RFID Mutual Authentication Protocol: SASI using Recursive hash", International Journal of Distributed Sensor Networks Vol. 2016 (2016), Article ID 9648971, 14 pages. doi:10.1155/2016/9648971 (IF-0.665)
4. Umar Mujahid and M. Najam-ul-Islam, "KMAP: A New Ultralightweight RFID Authentication Protocol for passive low cost tags," Wireless Personal Communications (WPC) Springer (Accepted with minor Revisions) (IF 0.67)
5. Umar Mujahid, Rizwan Aamir and M. Najam-ul-Islam "Cryptanalysis of Ultralightweight Mutual Authentication Protocols", ETRI Journal (Under Review).
6. Umar Mujahid and M. Najam-ul-Islam, "Pitfalls in Ultralightweight RFID Authentication Protocol", International Journal of Communication Networks and Information Security, Vol. 7, No. 3, December 2015 (IF-0.65).
7. Umar Mujahid and M. Najam-ul-Islam," Probabilistic recursive cryptanalysis of ultralightweight mutual authentication protocols for passive RFID systems", Pakistan Journal of Engineering and Applied Sciences (PJEAS), Article ID-388, (Article in press).
8. Umar Mujahid, M. Najam-ul-Islam, "Ultralightweight cryptography for passive RFID systems", International Journal of Communication Networks and Information Security, Vol.6. No.3, December 2014 (IF-0.65.)
9. Meena Nawaz, Umar Mujahid et.al," RFID: Design Parameters and Security Issues" World Applied Sciences Journal Vol.23, No.2, ISSN: 1818 – 4952, 2013.
10. Muhammad Zubair, Umar Mujahid, M. Najam-ul-Islam and Jameel Ahmed, "Cryptanalysis of RFID Ultra-lightweight Protocols and comparison between its Solutions Approaches", BU Journal of Information and Communication Technologies Vol. 5, Issue 1, 2012.

Conferences

11. Umar Mujahid, Yusra Mehmood, M. Najam-ul-Islam, Atif Raza Jafri, "Efficient Hardware Implementation of Lightweight Pseudorandom number generators", 2nd International Conference on Computer Science, Engineering and Educational Technologies (CSCEET-2015), September 8-10, 2015, Kuala Lumpur, Malaysia.
12. Umar Mujahid and M. Najam-ul-Islam,"A novel pseudorandom number generator for passive RFID systems", 17th IEEE-International multi topic conference (INMIC-2014), December 8-10, 2014, Karachi Pakistan.

13. Qurat-Ul-Ain, Umar Mujahid, M. Najam-ul-Islam,” Cryptanalysis of Mutual Ultralightweight Authentication Protocols: SASI & RAPP”, 8th IEEE international Conference on Open Source Systems and Technologies (ICOSST-2014), Lahore Pakistan, December 17-19, 2014.
14. Qurat-ul-Ain, Umar Mujhaid, M. Najam –ul-islam,” Hardware Implementation of Ultralightweight Cryptographic Protocols”, International Conference on Computing, Communication and Security (ICCCS), December 4-6, 2015, Mauritius.

I dedicate this thesis to our Kind Holy Prophet Hazrat Muhammad ﷺ

In the name of Allah, the Beneficent, the Merciful.

Acknowledgements

First of all, I would like to thank Almighty Allah for His countless blessings bestowed upon myself. I would like to express my deepest gratitude to my supervisor, Prof. M. Najam-ul-Islam, who was not only a mentor but also an exceptional colleague and above all an outstanding friend. I cherish the long hours and countless nights spent with Prof. Najam working on this thesis during this time. His continuous support, guidance and encouragement helped me achieve this endeavor.

I am grateful to Dr. Atif Raza Jafri for helping me with some of the technical aspects of this thesis. I would like to thank Prof. Pedro Paris Lopez for his guidance in initiating this research. Prof. Lopez inspired me to undertake this research and his contributions to the field were the stepping stones for me during the early years of this research. I am also thankful to Dr. Muhammad Ali Shami for his guidance during this research. I would also like to thank my colleagues in the University and the administration staff for helping me during this time.

I express my special gratitude to Dr. Imran Siddiqi and Dr. Muhammad Muzammal for reviewing this thesis which certainly helped in making this thesis a more comprehensible document.

Finally, I would like to thank my parents for being the best parents in this world, my brothers, Hummad and Usman, for all the cheering during stress times, my wife for her love and patience during the long research hours and my beloved daughter, Irha, for all her cuteness and the happiness she has brought to my life. This research was not possible without the support, prayers and love from my family.

Thank you! ☺

Abstract

Radio Frequency Identification (RFID) is one of the most promising identification schemes in the field of pervasive systems. Non-line of sight capability makes RFID systems more protuberant than its contended systems (such as barcode, magnetic tape etc.). RFID systems mainly consist of three main components: tag, reader and the backend database. A tag is a small electronic chip (transponder) implanted on an object which needs to be identified. A reader scans the tags, collects identification information and forwards this information towards the backend database (server) for the final verification.

Security and privacy are the two major concerns of RFID based identification systems which are associated with the tag's cost. On the basis of the tag's cost and computational capabilities, the RFID tags can be classified into two types: high and low cost tags. Our research work focuses on low cost RFID tags. High cost tags are resourceful enough to support traditional cryptographic algorithms and primitives such as AES, hash functions, stream ciphers etc. for security. These conventional cryptographic algorithms and primitives have excessive power, memory and silicon (chip) area requirements; which are transcendent from the low cost tag's computational capabilities. Hence, a new field *ultralightweight cryptography* has been introduced to ensure the security of low cost RFID tags in recent years. Ultralightweight cryptography avoids the use of costly operations and supports only simple *T-functions* and some special purpose ultralightweight primitives for the security.

This research examines the security issues of low cost RFID systems and makes five contributions. First, we perform the security analysis of numerous *Ultralightweight Mutual Authentication Protocols* (UMAPs) and discuss the pitfalls in the design of these protocols. Secondly, we present a sophisticated security model to validate the security claims of the UMAPs and cryptanalyze four eminent UMAPs (EMAP, SASI, Yeh et al. and RAPP). We use Recursive Linear Cryptanalysis (RLC) on SASI protocol and quasi linear cryptanalysis on Yeh et al. to retrieve tag's secret *ID*. Further desynchronization and two Denial of Service (DoS) attacks on RAPP protocol have also been highlighted. Thirdly, we propose three new UMAPs (RCIA, SASI using Recursive Hash and KMAP) which are robust against all possible existing attacks. Moreover, a counter based methodology has also been assimilated with GOASSMER protocol and R^2AP to avoid multiple DoS attacks and traceability attacks. Since the proper hardware implementation of such UMAPs has been long neglected, hence it is unclear that whether such protocols are practically compatible with low cost RFID tags having limited on-chip hardware compatibility or not. We therefore present an efficient hardware implementation of proposed UMAPs for EPC-C1G2 tags using both FPGA and ASIC design flows as our fourth contribution. The simulation and synthesis results of the proposed optimized hardware architecture show the compatibility of the proposed UMAPs with extremely low cost RFID tags. The low cost RFID tags don't support conventional cryptographic primitives such as on-chip random number generators and conventional hash functions due to resource constraints. We propose two new primitives, *Rot* and *Recursive Hash*, to generate the Pseudorandom Numbers which result in Ultralightweight Pseudorandom Number Generators (UPRNGs). We analyze their performance analysis, statistical properties and the efficient hardware implementation to validate their practical feasibility with the low cost RFID tags.

Table of Contents

- List of Publications iii
- Acknowledgement vi
- Abstract vii
- List of Figures xii
- List of Tables xiv
- List of Notations xv
- List of Abbreviations xvi
- 1 Introduction..... 1
 - 1.1 Overview..... 1
 - 1.2 Motivation..... 2
 - 1.3 Contributions..... 3
 - 1.4 Thesis Organization 4
- 2 RFID systems..... 6
 - 2.1 Introduction..... 6
 - 2.2 RFID system Components 7
 - 2.2.1 RFID Tags..... 7
 - 2.2.2 RFID reader 8
 - 2.2.3 RFID server/backend database..... 8
 - 2.3 RFID System Interface 8
 - 2.3.1 Tag coupling communication methods 8
 - 2.3.2 Data encoding and modulation schemes 9
 - 2.3.3 Collision avoidance in RFID system 10
 - 2.3.4 Frequency Band Regulations 10
 - 2.4 Standardization of RFID systems 10
 - 2.4.1 ISO Standards 10
 - 2.4.1 EPCglobal Standards..... 11
 - 2.5 Applications of RFID systems 13
 - 2.6 Security analysis of RFID systems 14
 - 2.7 Summary..... 15

3	Ultralightweight Cryptography for RFID systems.....	16
3.1	Introduction.....	16
3.2	General Structure of UMAPs.....	17
3.3	UMAP family protocols.....	19
3.3.1	LMAP	19
3.3.2	M ² AP.....	22
3.3.2	EMAP	25
3.4	UMAPs using Non – Triangular Primitives.....	27
3.4.1	The SASI Protocol	27
3.4.2	The GOASSMER Protocol	30
3.4.3	The Yeh et al. Protocol	33
3.4.4	The RAPP Protocol.....	35
3.4.5	The RAPLT Protocol	39
3.4.6	The R ² AP Protocol.....	42
3.5	Summary	45
4	Proposed Security Frameworks for UMAPs.....	46
4.1	Introduction.....	46
4.2	Pitfalls in UMAP designs.....	47
4.3	Proposed Security Analysis Framework.....	49
4.3.1	Functionalities of the protocols.....	50
4.3.2	Security model/ attacks	50
4.4	Proposed Cryptanalysis.....	54
4.4.1	Full Disclosure Attack on EMAP	54
4.4.2	Full Disclosure Attack on SASI.....	55
4.4.3	Full Disclosure Attack on Yeh et al. Protocol.....	57
4.4.4	Cryptanalysis of RAPP Protocol.....	60
4.5	Summary	64
5	Proposed Ultralightweight Mutual Authentication Protocols.....	65
5.1	Introduction.....	65
5.2	RCIA Protocol	66
5.2.1	The protocol	67
5.2.2	Security Analysis of RCIA protocol	69
5.2.3	Randomness tests	77

5.3	KMAP Protocol	77
5.3.1	The protocol	77
5.3.2	Security Analysis of the KMAP protocol	80
5.3.3	Randomness tests	85
5.4	SASI Protocol using Recursive hash	85
5.4.1	The Protocol	87
5.4.2	Security Analysis of the SASI using Recursive hash protocol	88
5.4.3	Randomness tests	92
5.5	Patches for GOASSMER protocol	92
5.6	Performance Analysis of UMAPs	94
5.7	Summary	94
6	Efficient Hardware Implementation of UMAPs	96
6.1	Introduction	96
6.2	Generic Design and Hardware Architecture	97
6.2.1	Register Block	97
6.2.2	ALU Block	98
6.2.3	Finite State Machine (FSM)	103
6.3	Circuit Synthesis and Experimental Results	104
6.3.1	Hardware Implementation on FPGA	104
6.3.2	Hardware Implementation on ASIC	106
6.4	Reconfigurable Architecture for UMAPs	106
6.5	Summary	108
7	Lightweight Pseudo-Random Number Generators	109
7.1	Introduction	109
7.2	Lightweight PRNGs	110
7.2.1	Linear Congruential Generator (LCG)	110
7.2.2	Linear Feedback Shift Register (LFSR)	111
7.2.3	AKARI -X	112
7.2.4	LAMED PRNG	113
7.3	Proposed PRNGs	114
7.3.1	RL- PRNG	114
7.3.2	EL- PRNG	116
7.4	Randomness tests of PRNGs	116

7.5	Circuit Synthesis and Performance comparison of PRNGs	118
7.5.1	FPGA based Prototyping	118
7.5.2	ASIC Resources Estimation	118
7.6	Summary	119
8	Conclusions and Future Works	120
8.1	Conclusions	120
8.2	Future Work	121
	Bibliography	123
	Appendix A	134
	A.1 Observation 3 (Proof):	134
	Appendix B	135
	B.1 Formal Analysis of RCIA	135
	B.2 Formal Analysis of KMAP	136
	B.3 Formal Analysis of SASI using Recursive hash	137
	Appendix C	139

List of Figures

- 2.1 Block diagram of RFID Tag 7
- 2.2 Passive Backscattering Communication Model 9
- 2.3 Inductive Coupling Communication model 9
- 2.4 Electronic Product Code (EPC) data format 13

- 3.1 General Structure of RFID UMAPs 17
- 3.2 LMAP Protocol 20
- 3.3 M²AP Protocol 24
- 3.4 EMAP Protocol 26
- 3.5 SASI Protocol 29
- 3.6 GOASSMER Protocol 32
- 3.7 Yeh et al. Protocol 34
- 3.8 RAPP Protocol 37
- 3.9 RAPLT Protocol 40
- 3.10 R²AP Protocol 43

- 4.1 Proposed Security framework 49
- 4.2 Histogram of ID_{conjunction} Candidate 59
- 4.3 Success probability of proposed quasi linear attack 60
- 4.4 DoS attack on Tag 62
- 4.5 DoS attack on Reader 62

- 5.1 The Computation of Recursive hash (Example)..... 67
- 5.2 The RCIA Protocol 68
- 5.3 The Computation of pseudo-Kasami code 78
- 5.4 The KMAP Protocol 79
- 5.5 The SASI using Recursive hash protocol 87

- 6.1 General Hardware Architecture of UMAPs 97

6.2	ALU Hardware schematic for RCIA protocol	99
6.3	Rotation module (m – bit).....	99
6.4	Recursive hash module.....	100
6.5	ALU Hardware schematic for KMAP protocol.....	101
6.6	The pseudo- Kasami encoder	102
6.7	ALU Schematic for SASI using Recursive hash protocol	103
6.8	Generic Reconfigurable Architecture for UMAPs	108
7.1	Hardware Schematic for LCG.....	111
7.2	Hardware Schematic for LFSR	111
7.3	Pseudo-code of AKARI-1 and AKARI-2	112
7.4	Hardware Schematic for AKARI-X	113
7.5	Hardware Schematic for LAMED-PRNG	114
7.6	Pseudo-code of RL-PRNG.....	115
7.7	Hardware Schematic for RL-PRNG	115
7.7	Hardware Schematic for EL-PRNG	116

List of Tables

2.1 RFID Vs Barcode 6

2.2 Modulation and Coding Schemes for RFID systems 10

2.3 Major ISO RFID Standards 11

2.4 Description of ISO 18000 Standards 11

2.5 Specifications of various tag classes..... 12

3.1 Properties of low cost RFID Tags 16

3.2 Notations used in chapter – 3 18

4.1 XOR vs OR Operation..... 56

4.2 Notations used in SASI attack..... 57

4.3 Steps of proposed RLC attack..... 59

4.4 Changing A&D messages and Conjecturing B&E messages..... 64

5.1 Notations Used in GNY Logic Analysis..... 74

5.2 Randomness test of RCIA with ENT, Diehard and NIST..... 76

5.3 Randomness test of KMAP with ENT, Diehard and NIST..... 86

5.4 Randomness test of SASI Using Recursive hash with ENT, Diehard and NIST 93

5.5 Performance analysis of several UMAPs (Tag side) 95

6.1 Resources utilizations of proposed UMAP designs on FPGAs..... 105

6.2 Hardware results of proposed UMAPs (ASIC)..... 107

6.3 Comparison of our proposed UMAPs with PRNGs based UMAPs 107

7.1 Test results of PRNGs obtained with ENT, Diehard and NIST suits 117

7.2 Performance analysis of proposed PRNGs using FPGAs..... 118

7.3 Hardware implementation results of PRNGs on ASIC..... 119

List of Notations

\mathcal{T}	Tag
\mathcal{R}	Reader
R_h	Recursive hash
K_c	pseudo-Kasami code
\oplus	XOR (Exclusive OR)
\vee	OR
\wedge	AND
\parallel	Concatenation operation
Rec	Reconstruction operation
Rot	Circular left rotation
Per	Permutation
n_1, n_2	Random numbers
K_1, K_2	Session keys
hw	Hamming weight
\longrightarrow	Transmission message direction