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 to 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 Figures

List of Tables

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
$\|\|$	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