



**Ain Shams University**  
**Faculty of Computer & Information Sciences**  
**Computer Systems Department**

# **Efficient Cryptography for RFID Systems**

**a thesis submitted as a partial fulfillment of the requirements for the degree of  
Master of Science in Computer and Information Sciences.**

**By**

**Eslam Gamal Ahmed Abd-Allah**

B.Sc. in Computer and Information Sciences,  
Teacher Assistant in Computer Systems Department,  
Faculty of Computer and Information Sciences,  
Ain Shams University.

**Under Supervision of**

**Prof. Dr. Mohamed Hashem**

Head of Information Systems Department,  
Information Systems Department,  
Faculty of Computer and Information Sciences,  
Ain Shams University.

**Dr. Hossam El-Deen Mostafa Fahim**

Associate Professor,  
Computer Systems Department,  
Faculty of Computer and Information Sciences,  
Ain Shams University.

**Dr. Eman Shaaban**

Lecturer,  
Computer Systems Department,  
Faculty of Computer and Information Sciences,  
Ain Shams University.

**Cairo 2010**

# Acknowledgements

All praise and thanks to ALLAH, who provided me the ability to complete this work. I hope to accept this work from me.

I am grateful of *my parents* and *my family* who are always providing help and support throughout the whole years of study. I hope I can give that back to them.

I also offer my sincerest gratitude to my supervisors, *Prof. Dr. Mohamed Hashem, Dr. Hossam Fahim and Dr. Eman Shaaban* who have supported me throughout my thesis with their patience, knowledge and experience.

Finally, I would thank my friends and all people who gave me support and encouragement.

# Abstract

This thesis examines the security issues of Radio Frequency Identification (RFID) technology, one of the most promising technologies in the field of ubiquitous computing. Indeed, it may well transform identification processes. RFID technology offers many advantages over other identification systems.

RFID systems can be classified according to tag price, with distinction between high-cost and low-cost tags. Our research work focuses mainly on low-cost RFID tags.

Without the appropriate controls, attackers can perform unauthorized tag reading and clandestine location tracking of people or objects. Snooping is possible by eavesdropping on tag/reader communications.

From a purely theoretical point of view, standard cryptographic solutions may be a correct approach. However, standard cryptographic primitives are quite demanding in terms of circuit size, power consumption and memory size, so they make costly solutions for low-cost RFID tags. Lightweight cryptography is therefore a pressing need.

In this thesis we cryptanalyzed Gossamer protocol and concluded that Gossamer show significant security flaws. We develop a lightweight mutual authentication protocol after modifying Gossamer protocol and analyze our modifications against possible attacks.

This thesis proposes also a combined distance bound protocol with lightweight mutual authentication protocol resistant to many RFID attacks and conforming to low-cost RFID tag requirements. In this protocol, costly computations are only performed by the reader, and security related computations in the tag are restricted to very simple operations.

The hardware complexity of the proposed protocol was analyzed, reckoning 1.68K gates for implementation; so it can be implemented in low-cost RFID tags which have a maximum of 4k gates devoted to security functions.

# Table of Contents

|                                                       |           |
|-------------------------------------------------------|-----------|
| <b>Acknowledgements.....</b>                          | <b>1</b>  |
| <b>Abstract.....</b>                                  | <b>2</b>  |
| <b>List of Figures.....</b>                           | <b>7</b>  |
| <b>List of Tables.....</b>                            | <b>9</b>  |
| <b>List of Abbreviations.....</b>                     | <b>10</b> |
| <b>List of Publications.....</b>                      | <b>12</b> |
| <b>Chapter 1: Introduction.....</b>                   | <b>13</b> |
| 1.1 Introduction.....                                 | 14        |
| 1.2 RFID History.....                                 | 20        |
| 1.3 EPC Class-1 Generation-2.....                     | 23        |
| 1.4 RFID Issues.....                                  | 24        |
| 1.5 Problem Definition.....                           | 26        |
| 1.6 Objectives.....                                   | 27        |
| 1.7 Main Contributions.....                           | 28        |
| 1.8 Thesis Outline.....                               | 29        |
| <b>Chapter 2: Radio Frequency Identification.....</b> | <b>30</b> |
| 2.1 RFID System Components.....                       | 31        |
| 2.1.1 RFID Readers.....                               | 32        |
| 2.1.2 RFID Tags.....                                  | 33        |
| 2.1.3 Host Computer.....                              | 34        |
| 2.2 RFID Middleware.....                              | 34        |
| 2.3 Passive Communications Methods.....               | 37        |

## **Chapter 3: Lightweight Mutual Authentication Protocol for Low-cost RFID Tags.....39**

|                                                                                                 |    |
|-------------------------------------------------------------------------------------------------|----|
| 3.1 Introduction.....                                                                           | 40 |
| 3.2 A Minimalist Mutual-Authentication Protocol for Low-cost RFID Tags (M <sup>2</sup> AP)..... | 41 |
| 3.3 An Efficient Mutual-Authentication Protocol for Low-cost RFID Tags (EMAP) .....             | 43 |
| 3.4 Lightweight Mutual Authentication Protocol (LMAP).....                                      | 45 |
| 3.5 SASI Protocol.....                                                                          | 47 |
| 3.6 Gossamer Protocol.....                                                                      | 49 |
| 3.6.1 Cryptanalysis of SASI Protocol.....                                                       | 49 |
| 3.6.2 Gossamer Protocol.....                                                                    | 50 |
| 3.6.3 Security Analysis of Gossamer Protocol.....                                               | 51 |
| 3.6.4 Performance Analysis of Gossamer Protocol.....                                            | 53 |

## **Chapter 4: Distance Bound Protocols for RFID Systems.....54**

|                                                         |    |
|---------------------------------------------------------|----|
| 4.1 Introduction.....                                   | 55 |
| 4.2 Relay Attack.....                                   | 55 |
| 4.3 Hancke and Kuhn's Protocol.....                     | 56 |
| 4.4 Munilla, Ortiz, and Peinado Protocol .....          | 57 |
| 4.5 Distance Bound Protocol using Mixed Challenges..... | 58 |

|                                                                                                |           |
|------------------------------------------------------------------------------------------------|-----------|
| <b>Chapter 5: Proposed Lightweight Protocol for Low-cost RFID Tags.....</b>                    | <b>61</b> |
| <b>5.1 Proposed Lightweight Mutual Authentication Protocol for Low-cost RFID Tags.....</b>     | <b>62</b> |
| 5.1.1 Cryptanalysis of Gossamer Protocol.....                                                  | 62        |
| 5.1.2 Proposed Lightweight Mutual Authentication Protocol .....                                | 64        |
| 5.1.3 Analysis of Proposed Lightweight Mutual Authentication Protocol .....                    | 65        |
| <b>5.2 Combining Distance Bound Protocol with Proposed Mutual Authentication Protocol.....</b> | <b>66</b> |
| <b>5.3 Security Analysis of the Proposed Combined Protocol.....</b>                            | <b>68</b> |
| 5.3.1 RFID Attacks.....                                                                        | 68        |
| 5.3.2 Proposed Combined Protocol against RFID Attacks.....                                     | 75        |
| <b>5.4 State Diagram of the Proposed Combined Protocol.....</b>                                | <b>77</b> |
| <b>5.5 Block Diagram of Hardware Implementation.....</b>                                       | <b>78</b> |
| <b>5.6 VHDL Code for the Proposed Combined Protocol.....</b>                                   | <b>80</b> |
| <b>5.7 Implementation Results.....</b>                                                         | <b>86</b> |
| <b>Chapter 6: Conclusion and Future Work.....</b>                                              | <b>87</b> |
| 6.1 Conclusion.....                                                                            | 88        |
| 6.2 Future Work.....                                                                           | 89        |
| <b>GLOSSARY.....</b>                                                                           | <b>90</b> |
| <b>REFERENCES.....</b>                                                                         | <b>93</b> |
| <b>Arabic Summary.....</b>                                                                     | <b>1</b>  |

## List of Figures

|                                                                 |    |
|-----------------------------------------------------------------|----|
| Figure 1.1: Typical RFID system.....                            | 14 |
| Figure 1.2: HF Tag examples.....                                | 15 |
| Figure 1.3: UHF Tag examples.....                               | 16 |
| Figure 1.4: A sheep with an ear tag .....                       | 16 |
| Figure 1.5: RFID in timing race application.....                | 17 |
| Figure 1.6: Barcode VS. RFID tag.....                           | 18 |
| Figure 1.7: RFID VS. Barcode.....                               | 18 |
| Figure 1.8: Watson-Watt with the first radar apparatus.....     | 20 |
| Figure 1.9: Stop RFID.....                                      | 25 |
| Figure 2.1: Basic schematic of all RFID systems.....            | 31 |
| Figure 2.2: Examples of RFID readers.....                       | 32 |
| Figure 2.3: Examples of passive RFID tags.....                  | 34 |
| Figure 2.4: Examples of active RFID tags.....                   | 34 |
| Figure 2.5: Functional components in an RFID system.....        | 35 |
| Figure 2.6: Passive Backscatter.....                            | 37 |
| Figure 2.7: Inductive Coupling.....                             | 37 |
| Figure 3.1: M <sup>2</sup> AP Protocol.....                     | 42 |
| Figure 3.2: EMAP Protocol.....                                  | 44 |
| Figure 3.3: LMAP tag identification stage.....                  | 46 |
| Figure 3.4: LMAP mutual authentication stage.....               | 46 |
| Figure 3.5: SASI Protocol.....                                  | 48 |
| Figure 3.6: Gossamer Protocol.....                              | 50 |
| Figure 4.1: Distant fraud attack.....                           | 56 |
| Figure 4.2: Mafia and terrorist fraud attack.....               | 56 |
| Figure 4.3: Hancke and Kuhn's Protocol.....                     | 57 |
| Figure 4.4: Munilla, Ortiz, and Peinado Protocol.....           | 58 |
| Figure 4.5: Distance bound protocol using mixed challenges..... | 59 |

|                                                                                                                              |    |
|------------------------------------------------------------------------------------------------------------------------------|----|
| Figure 5.1: Proposed lightweight mutual authentication protocol at reader.....                                               | 64 |
| Figure 5.2: Proposed lightweight mutual authentication protocol at tag.....                                                  | 64 |
| Figure 5.3: Modified MixBits in proposed lightweight mutual authentication protocol.....                                     | 65 |
| Figure 5.4: Combined distance bound using mixed challenges with proposed lightweight mutual authentication protocol.....     | 67 |
| Figure 5.5: Distance bound protocol using mixed challenges based on proposed lightweight mutual authentication protocol..... | 67 |
| Figure 5.6: Classification of RFID attacks.....                                                                              | 68 |
| Figure 5.7: State diagram of proposed combined protocol.....                                                                 | 77 |
| Figure 5.8: Data path and controller in single purpose processor.....                                                        | 78 |
| Figure 5.9: Hardware implementation of proposed combined protocol.....                                                       | 79 |
| Figure 5.10: RTL schematic for proposed combined protocol.....                                                               | 79 |

## List of Tables

|                                                                                                                                    |    |
|------------------------------------------------------------------------------------------------------------------------------------|----|
| Table 1.1: RFID operating frequencies and associated characteristics.....                                                          | 15 |
| Table 1.2: RFID VS. Barcode.....                                                                                                   | 19 |
| Table 2.1: Active VS. Passive RFID Tags.....                                                                                       | 33 |
| Table 2.2: RFID middleware filter types.....                                                                                       | 35 |
| Table 2.3: RFID middleware aggregate types.....                                                                                    | 36 |
| Table 3.1: Low-cost RFID tags specifications.....                                                                                  | 40 |
| Table 5.1: Prevented attacks in proposed combined distance bound protocol with<br>lightweight mutual authentication protocol ..... | 76 |
| Table 5.2: Implementation results.....                                                                                             | 86 |

## List of Abbreviations

|                    |                                                     |
|--------------------|-----------------------------------------------------|
| ALU:               | Arithmetic Logic Unit                               |
| ASIC:              | Application-Specific Integrated Circuit             |
| DHS:               | Department of Homeland Security                     |
| DPA:               | Differential Power Analysis                         |
| EAN:               | European Article Number                             |
| EEPROM:            | Electrically Erasable Programmable Read-Only Memory |
| EMAP:              | Efficient Mutual-Authentication Protocol            |
| EPC:               | Electronic Product Code                             |
| EPC-C1G2:          | EPC Class-1 Generation-2 standard                   |
| FPGA:              | Field-Programmable Gate Array                       |
| FRAM:              | Ferroelectric Random-Access Memory                  |
| HF:                | High Frequency                                      |
| ICAO:              | International Civil Aviation Organization           |
| IDS:               | Index-pseudonym                                     |
| IFF:               | Identify Friend or Foe                              |
| ITF:               | Interrogator-Talk-First                             |
| LF:                | Low Frequency                                       |
| LUT:               | Look Up Table                                       |
| LMAP:              | Lightweight Mutual Authentication Protocol          |
| M <sup>2</sup> AP: | Minimalist Mutual-Authentication Protocol           |
| PHP:               | Hypertext Preprocessor                              |

---

|       |                                                                                 |
|-------|---------------------------------------------------------------------------------|
| RAM:  | Random Access Memory                                                            |
| RFID: | Radio Frequency Identification                                                  |
| ROM:  | Read-Only Memory                                                                |
| RTL:  | Register Transfer Level                                                         |
| SASI: | Strong Authentication and Strong Integration                                    |
| SPA:  | Simple Power Analysis                                                           |
| SQL:  | Structured Query Language                                                       |
| TID:  | Tag Identifier                                                                  |
| UHF:  | Ultra High Frequency                                                            |
| UMAP: | Ultralightweight Mutual Authentication Protocols                                |
| UPC:  | Universal Product Code                                                          |
| VHDL: | VHSIC hardware description language; VHSIC: very-high- speed integrated circuit |
| XML:  | Extensible Markup Language                                                      |

## List of Publications

[1] Eslam Gamal Ahmed, Eman Shaaban, Mohamed Hashem “Lightweight Mutual Authentication Protocol for Low cost RFID Tags”, International Journal of Network Security & Its Application (IJNSA), Academy & Industry Research Collaboration Center (AIRCC), April 2010, Vol.2, No.2, PP. 27-37, ISSN: Online - 0974 – 9330, ISSN: Print - 0975 - 2307.

[2] Eslam Gamal Ahmed, Eman Shaaban, Mohamed Hashem “Lightweight Distance Bound Protocol for Low cost RFID Tags”, International Journal of Computer Science and Information Security (IJCSIS), LJS Publisher and IJCSIS Press, United States, March 2010, Vol.7, No.3, PP. 62-67, ISSN: 1947-5500.

[3] Eslam Gamal Ahmed, Eman Shaaban, Mohamed Hashem “Lightweight Mix Columns Implementation for AES”, 9th WSEAS International Conference on APPLIED INFORMATICS AND COMMUNICATIONS (AIC '09), 20-22 August 2009, Moscow, Russia, PP. 253-258, ISSN: 1790-5109, ISBN: 978-960-474-107-6.

# **Chapter 1:**

## **Introduction**

The purpose of this chapter is to present a basic introduction of RFID systems, RFID history and EPC standard. It also explains the motivation, objectives and main contributions of this thesis.

## 1.1 Introduction

RFID stands for Radio Frequency Identification which is a means of identifying a person or object using a radio frequency transmission. The technology can be used to identify, track, sort or detect a wide variety of objects.

RFID systems improve efficiency in globalised supply chains but the implementation of the technology has been problematic. This is partly due to the manufacturing costs of tags, which are currently too high to justify widespread deployment across supply chains in the way that was originally imagined, and partly due to concerns over the potential for infringing the privacy of consumers who purchase RFID-tagged products. In addition, there are concerns about the health implications for staff employed in RFID-enabled workplaces, although this has not received as much attention in the press [16].

Communication occurs between a reader (interrogator) and a transponder (Silicon Chip connected to an antenna) often called a tag. Tags can either be active (powered by battery) or passive (powered by the reader field), and come in various forms including Smart cards, tags, labels, watches and even embedded in mobile phones.

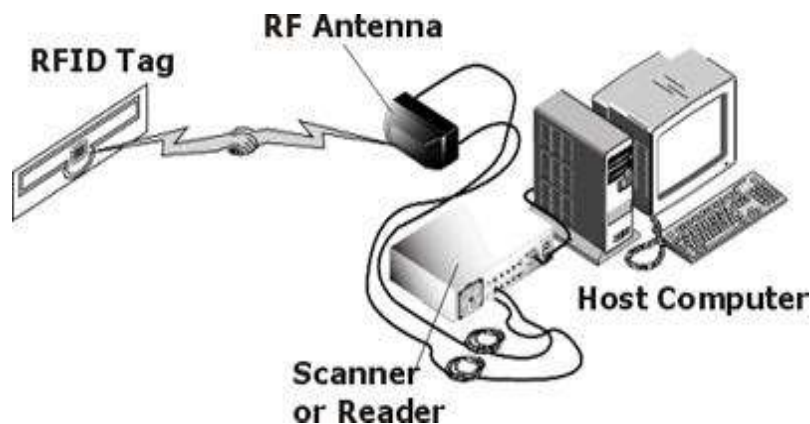


Figure 1.1 Typical RFID system

The communication frequencies used depends to a large extent on the application, and range from 125 KHz to 2.45 GHz. Regulations are imposed by most countries to control emissions and prevent interference with other Industrial, Scientific and Medical equipment (ISM) [24].