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

List of Figures

List of Tables

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^2AP:	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.

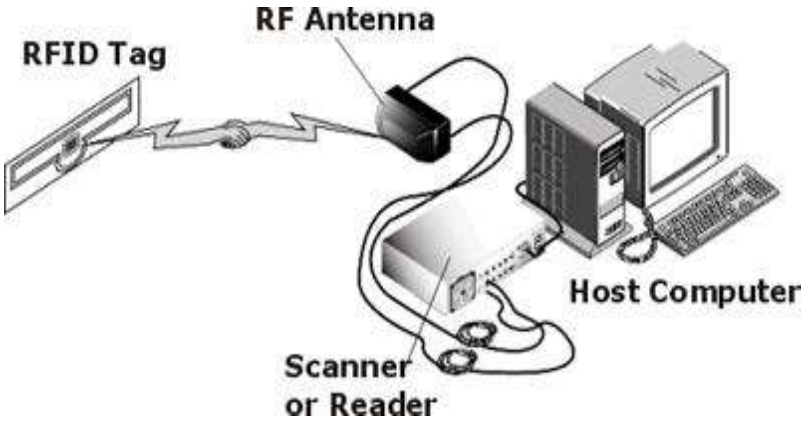

Figure 1.1 Typical RFID system

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].