RSA PERFORMANCE EVALUATION FOR PRIVACY PRESERVING SCHEME IN INTERNET OF THINGS.

BAHAREH MALEKI ALAVI

A project report submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

JANUARY 2013

This project report is dedicated to my family especially my mom and dad for their endless support and encouragement.

ACKNOWLEDGEMENT

First praise and thanks are for Allah who is guiding us continually and all the life especially for this graduating section .The one who is always available and hear our speaking then show the suitable way to human based on their requirements.

Upon the successful completion of this project, I would like to express my sincere thanks to Dr. Mohammad Abdur Razzaque, my supervisor, for his encouragement, guidance and advices. Thanks for all the time he spent for me along this project and showed me the way of researching.

My sincere appreciation also goes to Dr. Anazida Zainal who patiently listen to me and guided me where I need. At the end , my utmost thanks go to my parents and my whole family which are not near me but encourage me from my country in the whole graduating path specifically for this project and gave me the strength of face the different challenges.

ABSTRACT

A worldwide network of interconnected objects which are uniquely addressable, based on standard communication protocols is called: Internet of Things (IOT). As the Internet of Things is a large field with diverse technologies used there is a categorization of components including: Communication, sensors/RFID sensors, actuators, storage, devices, processing, localization and Tracking that each component has its own special problems of security which might be happened. The major factor which plays an important role in the future Internet of Things is Privacy. The protection of data and privacy of users is one of the key challenges in Internet of Things. Lack of confidence about privacy is one of the driving factors in the success of intelligent collaboration of miniaturized sensors. So it is needed to identify an applicable mechanism of privacy in internet of things. As RFID tags identify unique items and RFID market is growing fast and also RFID tags posing an important role in Internet of Things, various mechanisms exist for privacy. In this project evaluation of existing mechanisms in RFIDs has been considered and enhanced mechanism selected in this area. By using the Montgomery reduction for implementing the RSA algorithm and combing by hybrid method in multiplication, improvement in performance is achieved based on clock cycle counts.

ABSTRAK

Dalam satu rangkaian seluruh dunia antara objek yang saling berhubung di mana ianya dicapai dengan alamat yang unik, berdasarkan standard protokol komunikasi yang dipanggil: Perkara Internet (IOT). Diketahui bahawa Perkara Internet adalah satu bidang yang besar dengan pelbagai teknologi yang digunakan, setiap komponen mempunyai masalah keselamatan tersendiri yang mungkin berlaku. Faktor utama yang memainkan peranan penting dalam Perkara Internet pada masa hadapan adalah Peribadi (Privasi). Perlindungan terhadap data dan privasi pengguna adalah salah satu cabaran utama dalam Perkara Internet. Kekurangan dalam keyakinan terhadap privasi adalah salah satu faktor yang mendorong kejayaan dalam kerjasama pintar terhadap sensor miniaturi. Jadi ia diperlukan untuk mengenal pasti satu mekanisme berkenaan privasi dalam Perkara Internet. Diketahui bahawa tag RFID boleh mengenal pasti sesuatu barang yang unik dan pasaran RFID berkembang pesat dan tag RFID juga memainkan peranan penting dalam Perkara Internet, wujud pelbagai mekanisme untuk privasi. Dalam kes ini, penilaian projek terhadap mekanisme sedia ada dalam RFIDs telah diguna pakai dan mekanisme yang dipilih dipertingkatkan dalam bidang ini. Dengan menggunakan pengurangan Montgomery untuk melaksanakan algoritma RSA dan mengintegrasikan melalui kaedah hibrid dalam pendaraban, peningkatan dalam prestasi dicapai pada kiraan kitaran jam.

CHAPTER 1

INTRODUCTION

1.1 Introduction

In this chapter, a description of the background and statement of the problem for this project are presented. In continue, objectives of this project are illustrated. Then description for the scope and significance for this project is determined in separate sections clearly.

1.2 Background of the Study

In the first days of creation of ARPANET no one knew that this combination of four existing nodes will grow in this speed and at least such a great interconnected networks in all over the world will be developed. Networks which will be in high performance with capability of self-organizing in the future. As a statistic view, the population of people who use this World Wide Web network is increasing till they are now approximately 1.5 billion which is about 20% of the whole population of the world. Several reasons such as huge amount of people and end users all over the world, extent of various types of networks, production of advanced systems and devices with high computational performance and less amount of energy consumption bring out different styles of living which are new and lead us to have a

special trend to accept the concept which is addressed as Internet Of Things. The study in this field has started from 2006 and still continues because of need to connect smart manufactures and devices to each other. With development of smart manufactures, these smart objects can connect to the Internet and they can be remotely configured and updated, These benefits can be used in houses , offices, health care centers, transportation , animal protection , shopping centers and so on (Wang *et al*. 2010) .

As a result of connecting different objects to each other to obtain the Internet of Thing (IOT), several techniques may be used as enablers of IOT such as RFIDs. Radio Frequency Identification technology with specific capabilities will be used as one of the backbones of IOT. Due to low consumption of energy, low price and easy to implementation, use of RFID as an alternative to barcode is increasing and will continue in future. In the past RFID was only used in Retails and logistics but nowadays RFID tags are used in various positions such as payment services and transportations and in each position where an ID as identification makes a big role. Inside these interconnected networks beside sensors and different technologies, several issues will be faced. One of the most important issues because of the nature of IOT and existence of communication in such situation is security and privacy problem. If people do not get enough confidence about their personal information in such environment with new technologies they will not move forward to this new technology (Mayer 2009b ; Leusse *et al*. 2009).

A RFID system consists of RFID tag, RFID reader and a back end server. As RFID tag covers identification of unique devices, privacy issue will be raised. That’s why it is important to make an effort to solve privacy problem and prepare suitable security first before or in parallel of implementation to adapt people with IOT. There are several mechanisms of protecting security of RFID systems that we can categorize them in two big parts as physical mechanisms such as kill codes, faraday cage and blocker tag and second cryptographic methods which are known as Randomized Hash-Lock Protocol and Hash Chain based Protocols. Several studies have been done in this area and also some schemes have been proposed which have

their own attributes (Mayer 2009b ; Anon n.d,2009). These works require further investigation for better improvements.

1.3 Statement of the Problem

Internet of Things means "a worldwide network of interconnected objects uniquely addressable, based on standard communication protocols." As mentioned before IOT includes several technologies and is a wide area, There are a categorize set of components such as: Communication, sensors/RFID sensors, actuators, storage, devices, processing, localization and tracking. Each component may have its specific issue of security but as IOT penetrates our daily life things the most important problems is privacy which has been shown in the study.(Mayer 2009b) There are several types of attitude to RFID's world with different aspects. We can categorize studies done in this case to three ways as: technology, law and regulation and management (Tao and Peiran 2010). In the first area for enhancement of algorithms as a result there are several mechanisms for solving security problems.

For adapting people with the future IOT, it is needed to protect data and personal information in each component. Several studies in this area have been done and as a result some security frameworks and schemes have been proposed but it is still an open area because of the span of IOT and security aspects in this environment. So it is necessary to evaluate the existing mechanisms in this area and propose the best one and improve its capabilities (Anon, 2010).

1.4 Purpose of the Study

First purpose of this study is to review the concept of Internet of Things, attributes and its role in the future life and its components. Then it is concentrated on

RFID, one of enablers of IOT and study and evaluating their security mechanisms which provide privacy is done. In continue, it is aimed to improve the existing situation of privacy in this world to protect important information from probable threats.

1.5 Objectives of the Study

In this project, it is supposed to achieve to some specific objectives which are mentioned as below:

- To study IOT and identify RFIDs and privacy issues in this field.
- To analyze current mechanisms of solving the privacy issues in RFID in the IOT perspective to propose an enhanced mechanism.
- To introduce the optimized methods of implementing RSA algorithm using in that mechanism and compare the results for improving the performance.

1.6 Research Questions

Some important questions may be asked in this field as an Internet Of Things perspective which are like below:

- What are the main roles of security problems in success of implementation of IOT? Do they have any specific limitations?
- Why protect of personal information of end users and tracking of their activities which are using IOT, is so important?

- Will the proposed security mechanism cover all the existing gap and vulnerabilities? How much is the proposed mechanism reliable and confidence due evaluation?

1.7 Significance of the Study

The importance of this study is related to significance of Internet OF Things in the future life, where each object may connect to network and also to Internet. Therefore they can communicate with each other and needed information is gathered easily. As a result, it is viable to having control on objects remotely which may have important role in logistics, transportation, medical centers and drugs, shopping centers and specific smart objects for example at houses. But in this situation protecting personal information of people or objects from probable vulnerabilities will be so important. That is why having suitable privacy mechanisms for this critical situation is so needed.

1.8 Scope of the Study

In this project evaluation of the privacy issues in existing component of IOT is done and it is concentrated specifically on RFID as an enabler of IOT. The existing mechanisms of protecting privacy issues of RFID in the world of IOT is evaluated and then for improving the performance in the specific scheme, optimized methods for implementing RSA algorithm are compared .

1.9 Summary

In this chapter, the introduction in the problem statement and the objectives of this project is introduced then description in the significance of this project is done clearly based on the projects scopes and research questions.

Inside chapter 2, the literature review of this project is described then the research methodology of whole project is introduced in chapter 3. The selected scheme for privacy preserving and its different functionality steps are described in chapter 4. In continue the optimized methods for implementing the RSA encryption and also some obtained results are compared in chapter 5. The achievements of whole project and also limitations of this project are presented in chapter 6.

REFERENCES

Ji, Z. & Anwen, Q., 2010. The application of internet of things(IOT) in emergency management system in China. *2010 IEEE International Conference on Technologies for Homeland Security (HST)*, pp.139–142. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5655073.

A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S.C.S., 2005. Energy analysis of public-key cryptography for wireless sensor networks. *IEEE Computer Society Press*, pp.324–328.

J .Anon, 2010,An architecture based on Internet of Things to support mobility and security in medical environments.*IEEE concumer comunication and networking conference*

D.N. Duck,2009, Open Issues in RFID Security.*IEEE internet technology and secured transactions.*

Atmel Corporation, 8-bit ARVR Instruction Set. Available at: http://www.atmel.com/dyn/resources/prod documents/doc0856.pdf.

Atzori, L., Iera, A. & Morabito, G., 2010. The Internet of Things: A survey. *Computer Networks*, 54(15), pp.2787–2805. Available at: http://linkinghub.elsevier.com/retrieve/pii/S1389128610001568 [Accessed March 13, 2012].

Comba, P.G.,1990, Exponentiation cryptosystems on the IBM PC. *IBM Systems Journal*, 29(no 4), pp.526–538.

Corporation, H., IMPLEMENTATIONS OF MONTGOMERY MULTIPLICATION ALGORITHMS IN MACHINE.

C¸. K. Koc¸, T. Acar, 1996, Analyzing and comparing Montgomery multiplication algorithms. *IEEE Micro*, 16, pp.26–33.

Daly, A., & Marnane, W. (2002). Efficient architectures for implementing montgomery modular multiplication and RSA modular exponentiation on reconfigurable logic. Proceedings of the 2002 ACM/SIGDA tenth international symposium on Field-programmable gate arrays - FPGA '02, 40. doi:10.1145/503053.503055

Feng, H. & Fu, W., 2010. Study of Recent Development about Privacy and Security of the Internet of Things. *2010 International Conference on Web Information Systems and Mining*, pp.91–95. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5662804 [Accessed March 14, 2012].

Frederix, I., 2009. Internet of Things and radio frequency identification in care taking, facts and privacy challenges. *2009 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology*, pp.319–323. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5172467.

Gls, D.Q. et al., 2011. Proposed Embedded Security Framework for Internet of Things (IoT). , pp.1–5.

J. Großschadl, R. M. Avanzi, E. Savas¸, and S.T., 2005. Energy-efficient software implementation of long integer modular arithmetic. *Springer Verlag*, 3659, pp.75–90.

Juels, A., 2006. RFID Security and Privacy : A Research Survey. , 24(2), pp.381–394.

Knuth, D.E., 1998. *Seminumerical Algorithms* 3rd ed., ser. The Art of Computer Programming. Addison-Wesley, 1998, vol. 2..

Koc,C.K,1994, High-speed RSA implementation. Available at: ftp://ftp.rsasecurity.com/pub/pdfs/tr201.Pdf.

Leusse, P. De et al., 2009. Self Managed Security Cell, a Security Model for the Internet of Things and Services. *2009 First International Conference on Advances in Future Internet*, pp.47–52. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5223407 [Accessed March 6, 2012].

Li, H.W. and Q., 2006. Efficient implementation of public key cryptosystems on mote sensors. *Springer Verlag*, pp.519–528.

Liang, W. & Peiji, S., 2011. Research on the protection algorithm and model of personal privacy information in internet of thing. *2011 International Conference on E-Business and E-Government (ICEE)*, pp.1–4. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5881587.

Liu, J. & Yang, L., 2011. Application of Internet of Things in the Community Security Management. *2011 Third International Conference on Computational Intelligence, Communication Systems and Networks*, pp.314–318. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6005691 [Accessed March 26, 2012].

Liu, Z., Großschädl, J. & Kizhvatov, I., 2010. Efficient and side-channel resistant RSA implementation for 8-bit AVR microcontrollers. *Workshop on the Security* Available at: http://www.caad.arch.ethz.ch/noolab/files/external/conferences/IoT2010_proceedings/pdf/WS1/WS1_6. seciot2010_submission_12_final_v0.pdf [Accessed December 4, 2012].

Marten, B.,2008, Internet of Things in 2020.

Mayer, C.P., 2009a. Electronic Communications of the EASST Workshops der Wissenschaftlichen Konferenz Kommunikation in Verteilten Systemen 2009 (WowKiVS 2009) Security and Privacy Challenges in the Internet of Things Security and Privacy Challenges in the Internet of Thing. , 17.

Mayer, C.P., 2009b. Security and Privacy Challenges in the Internet of Things. , 17.

Montgomery, P.L.,1985, Modular multiplication without trial division. *Mathematics of Computation*, 44, pp.519–521.

N. Gura, A. Patel, A. S. Wander, H. Eberle, and S.C.S., 2004. Comparing elliptic curve cryptography and RSA on 8-bit CPUs. *Springer Verlag*, pp.119–132.

Ofman, A.A.K. and Y.P., 1963. Multiplication of multidigit numbers on automata. *Soviet Physics - Doklady*, 7(no 7), pp.595–596.

Oleshchuk, V., 2009. Internet of things and privacy preserving technologies. *2009 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology*, pp.336–340. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5172470.

Osaka, K. et al., 2006. An Efficient and Secure RFID Security Method. , pp.1090–1095.

Pateriya, R.K. & Sharma, S., 2011. The Evolution of RFID Security and Privacy: A Research Survey. *2011 International Conference on Communication Systems and Network Technologies*, pp.115–119. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5966417 [Accessed May 3, 2012].

R.L. Rivest, A.S.& L.M.A., 1978. A method for obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21(1978), pp.120–126.

Ryu, E.-K. & Takagi, T., 2009. A hybrid approach for privacy-preserving RFID tags. *Computer Standards & Interfaces*, 31(4), pp.812–815. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0920548908001104 [Accessed May 3, 2012].

Shen, G. & Liu, B., 2011. The visions, technologies, applications and security issues of Internet of Things. *2011 International Conference on E-Business and E-Government (ICEE)*, pp.1–4. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5881892.

Tao, H. & Peiran, W., 2010. Preference-Based Privacy Protection Mechanism for the Internet of Things. *2010 Third International Symposium on Information Science and Engineering*, pp.531–534. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5945162 [Accessed April 10, 2012].

W. Diffie and M.E. Hellman, New Directions in Cryptography. *IEEE Transactions on Information Theory*, (Nov 1976), pp.644–654.

Wang, K. et al., 2010. Research on security management for Internet of Things. *2010 International Conference on Computer Application and System Modeling (ICCASM 2010)*, (Iccasm), pp.V15–133–V15–137. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5622549.

Yang, J. & Fang, B., 2011. Security model and key technologies for the Internet of things. *The Journal of China Universities of Posts and Telecommunications*, 18(December), pp.109–112. Available at: http://linkinghub.elsevier.com/retrieve/pii/S1005888510601598 [Accessed May 3, 2012].

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	DECLARATION	ii
	DEDICATION	iii
	ACKNOWLEDGEMENT	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENT	vii
	LIST OF TABLES	xi
	LIST OF FIGURES	xii
1	**INTRODUCTION**	
1.1	Introduction	1
1.2	Background Of the study	1
1.3	Statement of the problem	3
1.4	Purpose of the study	3
1.5	Objectives of the Study	4
1.6	Research Questions	4
1.7	Significance Of the Study	5
1.8	Scope of the Study	5
1.9	Summary	6
2	**LITERATURE REVIEW**	
2.1	Introduction	7
2.2	Internet of Things (IOT)	7

2.2.1 Enablers of IOT 8

2.2.2 Architecture of IOT 10

2.2.3 The development of IOT 11

2.2.4 Categorization of components and sensitivity 11

2.3 RFID technology 12

2.4 The Use of RFID and IOT 13

2.5 RFID Attacks and Countermeasures 14

2.6 Privacy Issues 16

2.6.1 Preference-Based Privacy Protection Mechanism 17

2.6.2 A Cross Layer frame work for privacy enhancement in RFID 17

2.6.3 Three recent approaches 18

2.6.4 A Hybrid approach for privacy preserving RFID tags 18

2.7 Basic Multiplication Techniques 19

2.7.1 Schoolbook method 20

2.7.2 Comba's method 20

2.7.3 Karatsuba's method 20

2.7.4 Hybrid Multiplication 21

2.8 Montgomery modular Multiplication 21

2.9 Summary 23

3 RESEARCH METHODOLOGY

3.1 Introduction 25

3.2 Research Workflow 25

3.3 Respondents of the Study 25

3.4 Research Instruments Used 26

3.5 Data Analysis 27

3.6 Summary 28

4 ANALYSIS AND DESIGN

4.1 Introduction 29

4.2 RT scheme steps 29

4.3 Security analysis of RT scheme 29

4.4 Efficiency 32

4.5 Encryption method 34

4.6 Improve the Encryption implementation 34

4.7 Summary 34

5 IMPLEMENTATION METHOD EVALUATION

5.1 Introduction 36

5.2 Preliminaries 37

5.3 Modular Exponentiation 38

5.3.1 Flow chart of m-ary algorithm 39

5.4 Liu *et al* ‘s implementation method 40

5.4.1 Improved hybrid method 40

5.4.2 Hybrid Montgomery Multiplication 43

5.5 Wang *et al* ‘s implementation method 44

5.6 Wander et al 's implementation method 44

5.7 Performance evaluation of RSA algorithm implementation 45

5.8 Summary 46

6 DISCUSSION & CONCLUSION

6.1 Introduction 48

6.2 Discussion 48

6.3 Achievements 49

6.4 Limitations and Future works 49

6.5 Conclusion 50

REFERENCES 51

APPENDIX A 58

LIST OF TABLES

TABLE NO	TITLE	PAGE
5.1	Comparison of Instruction counts on the ATmega128	42
5.2	Performance of 1024-Bit RSA implementation	46

LIST OF FIGURES

FIGURE NO	TITLE	PAGE
2.1	Structure of a system in IOT perspective	11
2.2	Sensitivity of each component in IOT against security	12
2.3	The comparison between Hybrid scheme (RT) and other methods	19
2.4	Montgomery reduction algorithm	23
3.1	Workflow of process	25
4.1	Protocol setup phase	30
4.2	Protocol execution phase	31
5.1	M-ary method algorithm	38
5.2	The flowchart of m-ary algorithm	39
5.3	Register allocation between Original and new hybrid method	41
5.4	Comparison chart for instruction count between original and new hybrid method	42
5.5	HSOS integration view	43
5.6	The comparison chart based on clock cycle count	46