**IMPLEMENTATION OF SYMMETRIC ALGORITHM MODIFICATION SYSTEM TO RESIST POWER BASED SIDE CHANNEL ATTACKS**

Project Id: 039

Project Proposal Report

Pathirana K.P.A.P Lankarathne L.R.M.O Hangawaththa N.H.A.D.A

SUPERVISOR

…………………………………………………..

Mr. Kavinga Yapa Abeywardena

CO-SUPERVISOR

…………………………………………………..

Mr. Nuwan Kuruwitaarachchi

B.Sc. Special (Honors) Degree in Information Technology

Department of Information Technology

Sri Lanka Institute of Information Technology

March 2017

**DECLARATION**

We declare that this is our own work and this proposal does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other university or Institute of higher learning and to the best of our knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

|  |  |  |
| --- | --- | --- |
| Name | Student ID | Signature |
| Pathirana K.P.A.P | IT14120930 |  |
| Lankarathne L.R.M.O | IT14116216 |  |
| Hangawaththa N.H.A.D.A | IT14100376 |  |

The above candidates are carrying out research for the undergraduate Dissertation under my supervision.

.....………………………… ……………………

Signature of the supervisor: Date

**ABSTRACT**

Side channel attacks are the attacks based on “side channel information” which are the information that can be retrieved from the encryption device that is neither the plain text nor the cipher text resulting from the encryption process [1]. Side channel information are collected from heat, electromagnetic emissions, power consumption statistics etc… by these information we can determine information like the time that take for an operation and use these information to analyze an encryption algorithm to get information. At the present side channel attacks are getting much more popular since it is easy to mount an attack in a short time with only a few hundred dollars’ worth of devices and it is time saving comparing to other methods of breaking encryption also deep knowledge about algorithms isn’t required to perform an attack.

In present, publically available algorithms as well as customized algorithms are used for encryption purpose. There are no specific methods to determine whether these algorithms are vulnerable to a side channel attack and if it is what are those vulnerable points and necessary suggestions to overcome those vulnerabilities. Our objective is to design a system which collects power consumption values for algorithm and analyze those details to come up with possible algorithm modifications. As a result, that algorithm can be modified to mitigate the side channel attack risk. As a byproduct of this system, it provides a rating for the current position of the algorithm by running gathered data against a database which contains side channel information of popular and publically available asymmetric algorithms.

**TABLE OF CONTENTS**

Declaration of the candidate & Supervisor i

Dedication ii

Acknowledgements iii

Abstract iv

Table of content v

List of Figures vi

List of Tables vii

List of abbreviations viii

List of Appendices ix

1. Introduction 1

1.1 Section 1

1.2 Section 2

1.2.1 Sub Section 2

1.2.2 Sub Section 10

2. Title of the Chapter 17

3. Title of the Chapter 35

4. Title of the Chapter 57

5. Title of the Chapter 90

6. Conclusions and Recommendations 110

Reference List 125

Appendices

Appendix A: Title 130

Appendix B: Title 132

1. **INTRODUCTION**

**REFERENCES**

[1] Hagai Bar-Ei, “Introduction to Side Channel Attacks” [Online], Available: <http://gauss.ececs.uc.edu/Courses/c653/lectures/SideC/intro.pdf> [Accessed: March 12, 2017]