# PREFACE

Praise to God, the author dedicates this study to ALLAH SWT for His grace and His blessings, this thesis had been completed.

This thesis is a partial fulfillment of the requirements for the degree of Master of Informatics from the Informatics Postgraduate program at Telkom University.

I acknowledge that this thesis is still far from being perfect due to the various limitations that I should encounter. All advice and constructive criticism from everyone is highly expected for better achievements in the future. However I expect that this research is useful for all readers.

Bandung,

Farah Afianti

# Table Of Contents

APPROVAL i

SELF DECLARATION AGAINST PLAGIARISM ii

ABSTRACT iii

ABSTRAK iv

DEDICATION v

ACKNOWLEDGMENTS vi

PREFACE vii

TABLE OF CONTENTS viii

LIST OF TABLES x

LIST OF FIGURES xi

LIST OF ACRONYMS xii

1 THE PROBLEM 1

1.1 Rationale . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 1
1.2 Theoretical Framework . . . . . . . . . . . . . . . . . . . . . . . 2
1.3 Conceptual Framework/Paradigm . . . . . . . . . . . . . . . . . . 3
1.4 Statement of the Problem . . . . . . . . . . . . . . . . . . . . . 3
1.5 Hypothesis . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4
1.6 Assumption . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4
1.7 Scope and Delimitation . . . . . . . . . . . . . . . . . . . . . . 4
1.8 Importance of the Study . . . . . . . . . . . . . . . . . . . . . . 5

2 REVIEW OF LITERATURE AND STUDIES 6

2.1 Related Literature . . . . . . . . . . . . . . . . . . . . . . . . . 6
2.1.1 Mifare RFID Tag . . . . . . . . . . . . . . . . . . . . . . 6
2.1.2 Crypto-1 Cipher . . . . . . . . . . . . . . . . . . . . . . 7
2.1.3 Crypto-1 Authentication . . . . . . . . . . . . . . . . . . 8
2.1.4 Tag Nonce($n_T$) . . . . . . . . . . . . . . . . . . . . . . 10
2.1.5 Algebraic Attack . . . . . . . . . . . . . . . . . . . . . . 10

2.1.5.1 Multivariate Quadratic Problem . . . . . . . . . . . . . 16
2.1.5.2 Grain of Salt . . . . . . . . . . . . . . . . . . . . . . . 18
2.1.5.3 SAT Solver . . . . . . . . . . . . . . . . . . . . . . . 20
2.1.5.4 CryptominiSAT . . . . . . . . . . . . . . . . . . . . . 21
2.2 Related Studies . . . . . . . . . . . . . . . . . . . . . . . . . . . 24
2.2.1 Cryptography Properties On Boolean Function . . . . . . . . . . 24
2.2.2 Boolean Function Construction using Primitive Polynomial . . . . 27
2.2.3 Factorization and Common Subexpression Elimination . . . . . . 28

**3 RESEARCH METHODOLOGY 31**
3.1 Research Design . . . . . . . . . . . . . . . . . . . . . . . . . . . 31
3.1.1 System Implementation . . . . . . . . . . . . . . . . . . . . . 32
3.1.1.1 Wang Construction . . . . . . . . . . . . . . . . . . . 32
3.1.1.2 Cryptographic Properties Calculation . . . . . . . . . . 34
3.1.1.3 Factorization and Common Subexpression Elimination . 38
3.1.2 Implementation of Modified Crypto-1 Feedback Function . . . . . 39
3.1.3 Experiment Scenario . . . . . . . . . . . . . . . . . . . . . . . 41
3.2 Population/Sampling . . . . . . . . . . . . . . . . . . . . . . . . . 43
3.3 Instrumentation and Data Collection . . . . . . . . . . . . . . . . . 44
3.4 Tools for Data Analysis . . . . . . . . . . . . . . . . . . . . . . . 45

**4 PRESENTATION, ANALYSIS AND INTERPRETATION OF DATA 46**
4.1 Presentation of Data . . . . . . . . . . . . . . . . . . . . . . . . . 46
4.2 Analysis of the Data . . . . . . . . . . . . . . . . . . . . . . . . . 51
4.3 Summary of Findings . . . . . . . . . . . . . . . . . . . . . . . . 61

**5 CONCLUSIONS AND RECOMMENDATIONS 64**
5.1 Conclusions . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 64
5.2 Future Works . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 65

**Bibliography 66**

**Appendix A Grain of Salt Result 69**

**Appendix B The Example of Cryptography Properties Calculation 82**

**Appendix C Modified Feedback Boolean Function 85**

**Appendix D Curriculum Vitae 88**