

TABLE OF CONTENT

CHAPTER	TITLE	PAGE
	ABSTRACT	v
	LIST OF TABLE	xi
	LIST OF FIGURE	xii
	LIST OF APPENDIX	xiii
	LIST OF ABBREVIATIONS	xivi
I	INTRODUCTION	1
	1.1 Background	1
	1.2 Problem Statement	2
	1.3 Project Objectives	3
	1.4 Project Aim	3
	1.5 Project Scope	3
	1.6 Significant Of The Project	4
II	LITERATURE REVIEW	5
	2.1 Introduction	5
	2.2 Stream Ciphers	6
	2.3 Linear Feedback Shift Register (LSFR)	9
	2.4 Boolean Function	10
	2.5 Algebraic Attack	10
	2.6 Fast Algebraic Attack	11
	2.7 Algebraic Immunity	12
	2.8 Algorithm for Lowest Degree Computation	13
	2.9 Some sample of algebraic attack done by cryptanalyst	14
	2.9.1 SFINKS algorithm	14

CHAPTER	TITLE	PAGE
	2.9.2 WG algorithm	14
	2.10 Summary	15
III	METHODOLOGY	16
	3.1 Introduction	16
	3.2 Plan & Requirement Analysis	16
	3.3 Design and Build Tools for Evaluation	17
	3.3.1 Define method of evaluation	17
	3.3.2 Define method of observation and testing	17
	3.3.3 Design the application framework	17
	3.3.4 Design the physical model of tools	17
	3.3.5 Build the application	18
	3.4 Run the testing and obtain the test-run result	18
	3.4.1 Prepare the testing procedure	18
	3.4.2 Select the stream ciphers algorithm to be tested	18
	3.4.3 Run the test	18
	3.5 Result and Conclusion	19
	3.5.1 Prepare the testing report and findings	19
	3.6 Summary	19
IV	SYSTEM DESIGN	20
	4.1 Introduction	20
	4.2 Assumption and Theorem Bonded	20
	4.3 Finding the Existence of Annihilators (Algebraic Immunity, AI)	21
	4.3.1 Relation between n and $dg, dh - R$	22
	4.3.2 Relation between df and $dg, dh - R$	22
	4.3.3 Relation between AI and $dg, dh - R$	22
	4.3.4 Formula to calculate the data complexity	23
	4.3.5 Formula to calculate the time complexity	24
	4.4 Evaluation Process Framework	24

CHAPTER	TITLE	PAGE
	4.4.1 Relation Search Step	24
	4.4.2 Pre-Computation Step	25
	4.4.3 Substitution Step	25
	4.4.4 Solving Step	25
	4.4.5 Benchmark result	26
4.5	Summary	26
V	SYSTEM DEVELOPMENT	28
5.1	Introduction	28
5.2	Application Environment	29
	5.2.1 The Main Application Environment	29
5.3	Cryptographic Boolean Functions	30
	5.3.1 Algebraic Degree	30
	5.3.2 Binomial Coefficient	31
	5.3.3 Algebraic Immunity	31
5.4	Development of the Evaluation Model	32
	5.4.1 Relation search step	33
	5.4.2 Pre-computation step	35
	5.4.3 Substitution step	37
	5.4.4 Solving step	38
	5.4.5 Main Function	39
5.5	Summary	39
VI	TESTING AND RESULT	42
6.1	Introduction	42
6.2	SFINKS	42
	6.2.1 Description of SFINKS	43
	6.2.2 Getting the Algebraic Immunity Value	43
	6.2.3 Evaluation based on Framework	44
	6.2.4 Results Summary	46
6.3	WG	47
	6.3.1 Description of WG	47

CHAPTER	TITLE	PAGE
	6.3.2 Basic Properties Value	47
	6.3.3 Evaluation based on Framework	49
	6.3.4 Results Summary	50
VII	CONCLUSION	51
	7.1 Introduction	51
	7.2 Discussion	51
	7.3 Future work	53
	7.4 Conclusion	53
	REFERENCES	53
	APPENDIX A-B	56-92

LIST OF TABLE

TABLE NO	TITLE	PAGE
4.1	Logarithm of complexities of the algebraic attack	26
4.2	Logarithm of complexities of the fast algebraic attack	26
6.1	Value Recorded by tool compare to SFINKS Cryptanalysis Report	44
6.2	log ₂ complexities of FAA of SFINKS [2]	46
6.3	Value Recorded by tool compare to WG Cryptanalysis Report	48
6.4	log ₂ of complexities of FAA of WG [2]	50

LIST OF FIGURE

FIGURE NO	TITLE	PAGE
2.1	Communication Scheme with a symmetric primitive	6
2.2	General structures of a synchronous stream ciphers	8
5.1	Main Application Screen	29
5.2	Execution of MValue(n, d)	34
5.3	Execution of DataComplexity(n,dg,dh)	35
5.4	Execution of PrecompStep(n,dh)	36
5.5	Execution of SubsTep(n,dg,dh)	38
5.6	Execution of SolveStep(n, dg)	39
5.7	Execution of MaxComplexity(n, dg, dh) – Overall Complexity	41
6.1	Getting the AI for SFINKS	44
6.2	Execution Result of Relation Search for SFINKS	45
6.3	Getting the AI for WG	48
6.4	Execution result of Relation Search for WG	49

LIST OF APPENDIX

APPENDIX	TITLE	PAGE
A	Express User Manual	56
B	Source code	60

LIST OF ABBREVIATIONS

AI	-	Algebraic Immunity
AA	-	Algebraic Attack
FAA	-	Fast Algebraic Attack
IS	-	Information Systems
LSFR	-	Line Feedback Shift Register
OTP	-	One Time Pad
VB	-	Visual Basic