

# Contents

<b>ACKNOWLEDGEMENTS</b>	<b>iii</b>
<b>LIST OF TABLES</b>	<b>iv</b>
<b>ABBREVIATIONS</b>	<b>v</b>
<b>LIST OF SYMBOLS</b>	<b>vi</b>
<b>ABSTRACT</b>	<b>vii</b>
<b>1 INTRODUCTION</b>	<b>1</b>
1.1 Motivation . . . . .	4
1.2 Organization of the Thesis . . . . .	9
<b>2 PÓLYA’S ENUMERATION THEOREM</b>	<b>10</b>
2.1 Introduction . . . . .	10
2.2 Groups . . . . .	11
2.3 Group Action . . . . .	13
2.4 Cycle Index Polynomial . . . . .	15
<b>3 CRYPTOGRAPHIC BOOLEAN FUNCTIONS</b>	<b>18</b>
3.1 Introduction . . . . .	18
3.2 Representation of Boolean Functions . . . . .	18
3.2.1 Truth Table and Polarity Truth Table . . . . .	19
3.2.2 Algebraic Normal Form . . . . .	20
3.2.3 Trace Representation . . . . .	21
3.3 Tools for Analyzing Boolean Functions . . . . .	22
3.3.1 Walsh-Hadamard Transform . . . . .	22
3.3.2 Autocorrelation Spectrum . . . . .	24
3.4 Cryptographic Properties of Boolean functions . . . . .	25
3.4.1 Balancedness . . . . .	25
3.4.2 Nonlinearity . . . . .	25
3.4.3 Correlation Immunity and Resilience . . . . .	29
3.4.4 Avalanche Characteristics . . . . .	29
3.4.5 Algebraic Immunity . . . . .	31
3.5 Bounds and Relations on Complexity Measures . . . . .	32

3.5.1	Bounds on Nonlinearity . . . . .	32
3.5.2	Tradeoff Between Nonlinearity and Algebraic Immunity . . . . .	33
3.5.3	Tradeoff Between Nonlinearity and Avalanche Criterion . . . . .	34
3.5.4	Tradeoff Between Nonlinearity and Correlation Immunity . . . . .	35
<b>4</b>	<b>ROTATION SYMMETRIC FUNCTIONS</b>	<b>37</b>
4.1	Introduction . . . . .	37
4.2	Rotation Symmetric Boolean Functions . . . . .	38
4.3	Enumeration of Rotation Symmetric Boolean Functions . . . . .	40
4.4	Rotation Symmetric Functions over Finite Fields . . . . .	43
4.5	Weight and Nonlinearity of Homogeneous Rotation Symmetric Boolean Functions . . . . .	47
4.6	Enumeration of Balanced Rotation Symmetric Boolean Functions . . . . .	49
<b>5</b>	<b>AFFINE EQUIVALENCE OF ROTATION SYMMETRIC BOOLEAN FUNCTIONS</b>	<b>54</b>
5.1	Affine Equivalence of Boolean Functions . . . . .	55
5.2	Affine Equivalence of Quadratic MRS Boolean Functions . . . . .	56
5.3	Affine Equivalence of Cubic MRS Boolean Functions . . . . .	58
5.4	Affine Equivalence of Quartic MRS Boolean Functions . . . . .	60
5.5	Affine Equivalence of MRS Functions of Degree $d$ . . . . .	61
5.6	Cycle Index Polynomial of the Group $G$ . . . . .	63
<b>6</b>	<b>GENERALIZED ROTATION SYMMETRIC BOOLEAN FUNCTIONS</b>	<b>70</b>
6.1	Introduction . . . . .	70
6.2	$k$ -Rotation Symmetric Boolean functions . . . . .	71
6.3	Enumeration of $k$ -Rotation Symmetric Boolean Functions . . . . .	72
6.4	Weight and Nonlinearity of Quadratic 2-MRS Functions . . . . .	73
6.5	Rotation Symmetric S-boxes . . . . .	76
<b>7</b>	<b>CONCLUSIONS AND SCOPE FOR FUTURE WORK</b>	<b>80</b>
7.1	Conclusions . . . . .	80
7.2	Related Open Problems . . . . .	81
	<b>REFERENCES</b>	<b>82</b>
	<b>LIST OF PUBLICATIONS BASED ON THE RESEARCH WORK</b>	<b>91</b>