

CONTENTS

Abstract	II
Acknowledgments	III
List of Algorithms	VII
List of Figures	VIII
List of Tables	IX
List of Abbreviations	X
List of Symbols	XI
1 Introduction	1
2 Elliptic Curves	10
2.1 Weierstrass Equations.....	10
2.2 The Group Law	17
2.3 Addition Formulas	20
2.4 Elliptic Curves over Finite Fields	26
2.5 Counting the number of points	30
2.6 Discrete Logarithm Problem for Elliptic Curves.....	31
2.6.1 Known Algorithms	32
2.6.2 Weak Curves.....	33
2.7 Optimizing ECC Implementations.....	33
2.7.1 Domain Parameters.....	34
2.7.2 Coordinate Systems	37
2.7.3 Exponentiation	38
3 Elliptic Curve Exponentiation	39

3.1	Base-2 Representations of Integers.....	39
3.1.1	Signed Binary Representation	41
3.2	Algorithms for Elliptic Curve Exponentiation.....	43
3.2.1	Binary Methods.....	44
3.2.2	Sliding Window applied on NAF	49
3.2.3	The width- w Non Adjacent Form (w NAF).....	52
3.2.4	The width- w Mutual opposite Form (w MOF)	54
4	Contribution of This Thesis	63
4.1	Direct Computation of $2^{n_2} (2^{n_1} P + Q)$ in affine coordinate	63
4.1.1	The Break-Even Point.....	71
4.2	Exponentiation with Direct Computation of $2^{n_2} (2^{n_1} P + Q)$	73
4.2.1	Complexity Analysis of the w MOF Method	74
4.3	Implementation and Results.....	78
4.3.1	Elliptic Curves domain parameters and Platforms	78
4.3.2	Timings analysis of w MOF Exponentiation Method.....	79
5	Conclusion	83
	Appendix A Mathematical Background	85
A.1	Basic Algebra.....	85
A.2	Projective Space.....	87
	Appendix B	89
B.1	Recommended NIST Elliptic Curves over Prime Fields	89
B.2	Complete Java code.....	90
	Bibliography	100