

Contents

1	Introduction	1
1.1	Motivation	1
1.2	The contributions of this thesis.....	2
1.3	Thesis Organisation.....	2
2	Background	3
2.1	Finite-Field Arithmetic	3
2.2	Elliptic Curve Arithmetic	3
2.3	Scalar Multiplication	5
2.4	Summary.....	6
3	Review of literature	7
3.1	Generic-Point Parallel Scalar Multiplication Method	7
3.2	Efficient and Scalable Postcomputation-Based Generic-Point Parallel Scalar Multiplication Method.....	9
3.3	Highly Efficient Generic-Point Parallel Scalar Multiplication Using Concurrent Precomputations	11
3.4	High-Performance Generic-Point Parallel Scalar Multiplication	13

3.5	Summary	16
4	Methodology	17
4.1	Analysis	17
4.2	Implementation	19
4.3	Summary	20
5	Results	24
5.1	Performance Analysis	24
5.1.1	Finding the best method	25
5.1.2	New method	26
5.2	Discussion of the Results	26
5.3	Summary	39
6	Conclusion	40