

Contents

1	Introduction	1
1.1	Problem Statement and Motivation	1
1.2	Structure of the Thesis	3
2	Elliptic Curve Cryptography	5
2.1	Cryptography for Flash Memory Controllers	5
2.2	Applications of Elliptic Curve Cryptographic (ECC) Systems	7
2.3	Elliptic Curve Point Multiplication	14
2.4	Elliptic Curve Geometry and Group Laws	17
2.5	Reducing the Number of Field Inversions for Elliptic Curves over Prime Fields	20
2.6	Discussion	22
3	Elliptic Curve Cryptography over Gaussian Integers	25
3.1	Gaussian Integer Rings and Fields	26
3.2	Point Multiplication over Gaussian Integers	29
3.3	Resistance Against side Channel Attacks using Gaussian Integers	33
3.4	Discussion	41
4	Montgomery Arithmetic over Gaussian Integers	43
4.1	Montgomery Arithmetic	44
4.2	Reduction over Gaussian Integers using the Absolute Value	46
4.3	Reduction over Gaussian integers using the Manhattan Weight	51
4.4	Simplifying the Reduction based on the Manhattan Weight	57
4.5	Discussion	59

5	Architecture of the ECC Coprocessor for Gaussian Integers	61
5.1	Coprocessor Architecture for Gaussian Integers	62
5.2	ECC Coprocessor Architecture for Prime Fields	70
5.3	Implementation Results	76
5.4	Discussion	81
6	Compact Architecture of the ECC Coprocessor for Binary Extension Fields	83
6.1	Group Laws and Projective Coordinates for Binary Extension Fields	84
6.2	ECC Coprocessor Architecture	87
6.3	Results and Discussion	94
7	The Parallel Dictionary LZW Algorithm for Flash Memory Controllers	97
7.1	Data Compression for Flash Memory Devices	99
7.2	Parallel Dictionary LZW (PDLZW) Algorithm	107
7.3	Address Space Partitioning for the PDLZW	112
7.4	Reducing the Memory Requirements of the PDLZW	116
7.5	Compression and Implementation Results	124
7.6	Discussion and Comparison with Other Data Compression Schemes	128
8	Conclusion	131
	Bibliography	133