

Table of Contents

Abstract	iii
Kurzdarstellung	v
Preface	vii
1 Introduction	1
1.1 Security Requirements and Techniques	2
1.1.1 Public-Key Cryptography	3
1.1.2 Elliptic Curve Cryptography (ECC)	5
1.2 Thesis Outline	6
2 Mathematical Background	9
2.1 Introduction to Elliptic Curves	9
2.2 Elliptic Curve Parameter Selection	10
2.3 Elliptic Curve Arithmetic over \mathbb{F}_p	11
2.3.1 Field Arithmetic over \mathbb{F}_p	13
2.4 Elliptic Curve Arithmetic over \mathbb{F}_{2^m}	17
2.4.1 Field Arithmetic over \mathbb{F}_{2^m}	18
2.5 Elliptic Curve Arithmetic over \mathbb{F}_{p^m}	22
2.5.1 Field Arithmetic over Optimal Extension Fields (OEF)	23
2.6 Elliptic Curve Point Multiplication	27
2.6.1 Binary Method	28
2.6.2 Non-Adjacent Form (NAF) Method	28
2.6.3 Windowing Methods	28
2.6.4 Montgomery Method	29
2.7 Elliptic Curve Key Exchange and Signature Protocols	30
2.7.1 Elliptic Curve Diffie-Hellman Key Exchange	30

2.7.2	Elliptic Curve Digital Signature Algorithm	31
3	Software Design: ECDH Key Exchange on an 8-bit Processor	32
3.1	Motivation and Outline	32
3.2	Related Work	33
3.3	The Chipcon Architecture	33
3.4	Elliptic Curve Parameter Selection	33
3.5	Implementation aspects on the Chipcon processor	34
3.5.1	Field Arithmetic	34
3.5.2	Point Arithmetic	36
3.6	Communication Protocol	37
3.6.1	Key Establishment Phase	38
3.6.2	Normal Mode	39
3.7	Demonstration Application	39
3.8	Summary	41
4	Hardware/Software Co-design: Extensions for an 8-bit Processor	42
4.1	Motivation and Outline	42
4.2	Related Work	43
4.3	The FPSLIC Architecture	43
4.4	Implementation aspects on the AVR processor	44
4.4.1	Field Arithmetic	45
4.4.2	Point Arithmetic	46
4.5	Proposed Instruction Set Extensions	46
4.5.1	8-by-8 Bit-Parallel Multiplier	49
4.5.2	163-by-163 Bit-Serial Multiplier	49
4.5.3	163-by-163 Digit Serial Multiplier	50
4.5.4	A Flexible Multiplier	51
4.6	Summary	52
5	Hardware/Software Co-design: Extensions for a 32-bit Processor	56
5.1	Motivation and Outline	56
5.2	Related work	57
5.3	The MIPS32 architecture	58
5.4	Implementation aspects on the MIPS32 processor	59
5.5	Proposed extensions to MIPS32	61
5.5.1	Multiply/accumulate unit with a 72-bit accumulator	62

5.5.2	Custom instructions	63
5.5.3	Implementation details and performance evaluation	63
5.6	Summary	66
6	Hardware Design: Optimal Digit Multipliers for \mathbb{F}_{2^m}	67
6.1	Motivation and Outline	67
6.2	Background on Digit-Serial Multipliers.	68
6.3	Architecture Options for LSD	69
6.3.1	Single Accumulator Multiplier (SAM)	70
6.3.2	Double Accumulator Multiplier (DAM)	74
6.3.3	N-Accumulator Multiplier (NAM)	78
6.4	Evaluation of the Multiplier Options	79
6.4.1	Evaluation of the SAM	80
6.4.2	Evaluation of all multiplier options	82
6.5	Summary	83
7	Hardware Design: ECC in the Frequency Domain	86
7.1	Motivation and Outline	86
7.2	Mathematical Background	87
7.2.1	Number Theoretic Transform (NTT)	87
7.2.2	Convolution Theorem and Polynomial Multiplication in the Frequency Domain	88
7.3	Modular Multiplication in the Frequency Domain	89
7.3.1	Mathematical Notation	90
7.3.2	DFT Modular Multiplication Algorithm	90
7.3.3	Optimization	91
7.4	Implementation of an ECC Processor Utilizing DFT Modular Multiplication	94
7.4.1	Base Field Arithmetic	94
7.4.2	Extension Field Multiplication	95
7.4.3	Point Arithmetic	99
7.5	Performance Analysis	100
7.6	Summary	102
8	Hardware Design: Tiny ECC Processor over \mathbb{F}_{2^m}	106
8.1	Motivation and Outline	106
8.2	Mathematical Background	107

8.2.1	Squaring	108
8.2.2	Inversion	108
8.2.3	Point multiplication	110
8.3	Implementation Aspects	113
8.3.1	\mathbb{F}_{2^m} Adder Unit	113
8.3.2	\mathbb{F}_{2^m} Multiplier Unit	113
8.3.3	\mathbb{F}_{2^m} Squarer Unit	115
8.3.4	ECC Processor design	116
8.4	Performance Analysis	118
8.5	Summary	120
9	Discussion	123
9.1	Conclusions	123
9.2	Future Research	124
	Bibliography	126