

1	Introduction	5
2	Background	8
2.1	Algebraic structures	8
2.2	Cryptographic background	10
2.3	Environment of the experiments	13
3	Sequential exponentiation and addition chains	14
3.1	Exponentiation and q -addition chains	14
3.2	The algorithm of Brauer	19
3.3	Addition chains for sets	27
3.4	Experiments	29
4	Parallel exponentiation	34
4.1	An algorithm for parallel exponentiation	34
4.1.1	The depth of an addition chain with scalar	35
4.1.2	Basic algorithms	36
4.1.3	Parallelizing the non- q -steps	39
4.1.4	Collecting the results	41
4.1.5	Free scalar	44
4.2	A lower bound for parallel exponentiation	45
4.2.1	The basic idea	48
4.2.2	An extension to weighted addition chains	49
4.3	Consequence to parallel exponentiation	53
5	Polynomial bases	57
5.1	Polynomial arithmetic	57
5.2	Computing the canonical representative	61
5.2.1	Arbitrary modulus	62
5.2.2	Sparse polynomials	65
5.2.3	Sedimentary polynomials	72
5.3	Exponentiation in a polynomial basis representation	74
5.4	Division in a polynomial basis representation	75
6	Normal bases	79
6.1	Basics	79
6.2	The multiplication matrix	81
6.3	Optimal normal bases	85
6.4	Exponentiation in a normal basis representation	89
6.5	Division in a normal basis representation	90

7 Gauß periods	100
7.1 Definition of general Gauß periods	101
7.2 The condition $\langle q, \mathcal{K} \rangle = \mathbb{Z}_r^\times$	102
7.3 Cyclotomic polynomials	106
7.4 Field towers, traces, and normal elements	108
8 The prime power case	112
8.1 An algorithm for fast multiplication	112
8.2 Algorithms for division	132
8.3 Computation of the multiplication matrix	139
8.4 Normality of prime power Gauß periods	142
8.5 Exponentiation using normal prime power Gauß periods	143
9 Decomposable Gauß periods	145
9.1 Decomposition of Gauß periods	145
9.2 Fast multiplication for decomposable Gauß periods	149
9.3 Existence of decomposable Gauß periods	154
9.4 A criterion for the existence of a normal Gauß period	159
10 Scalable parallel exponentiation	164
10.1 A refined model	165
10.2 The main stage	168
10.3 Parallel precomputation	175
10.4 Experiments	184
11 Conclusions	192
A Appendix: Experiments	194
A.1 Addition chains	194
A.2 Basic arithmetic	204
A.2.1 Polynomial basis representation	204
A.2.2 Normal basis representation	208
A.2.3 Normal Gauß periods	212
A.3 Parallel exponentiation	222