



Universiteit
Leiden
The Netherlands

Computational aspects of class group actions and applications to post-quantum cryptography

Houben, M.R.

Citation

Houben, M. R. (2024, February 28). *Computational aspects of class group actions and applications to post-quantum cryptography*. Retrieved from <https://hdl.handle.net/1887/3721997>

Version: Publisher's Version

License: [Licence agreement concerning inclusion of doctoral thesis
in the Institutional Repository of the University of Leiden](#)

Downloaded from: <https://hdl.handle.net/1887/3721997>

Note: To cite this publication please use the final published version (if applicable).

Computational aspects of class group actions and applications to post-quantum cryptography

Proefschrift

ter verkrijging van
de graad van doctor aan de Universiteit Leiden,
op gezag van rector magnificus prof. dr. ir. H. Bijl,
volgens besluit van het college voor promoties
te verdedigen op woensdag 28 februari 2024
klokke 16.15 uur

door

Marcel Ronald Houben

geboren te Utrecht, Nederland

in 1995

Promotores:	Dr. T.C. Streng
	Prof. dr. P. Stevenhagen
Co-promotor:	Dr. W. Castryck
	(KU Leuven)
Promotiecommissie:	Prof. dr. N. Budur (KU Leuven)
	Prof. dr. ir. G.L.A. Derkx
	Dr. C.R. Martindale (University of Bristol)
	Dr. B.A. Smith (Inria / École polytechnique)
	Prof. dr. R.M. van Luijk

This work was carried out at Leiden University and KU Leuven, funded by Research Foundation – Flanders (FWO) through PhD Fellowship Fundamental Research 11C7322N.

Computational aspects of class group actions and applications to post-quantum cryptography

Marc Houben

Examination committee KU Leuven:

Supervisors:

Dr. Wouter Castryck	(KU Leuven)
Dr. Marco Streng	(Universiteit Leiden)
Prof. dr. Willem Veys	(KU Leuven)

Other members:

Prof. dr. Nero Budur	(KU Leuven)	Dissertation presented
Prof. dr. Ronald van Luijk	(Universiteit Leiden)	in partial fulfillment
Dr. Chloe Martindale	(University of Bristol)	of the requirements
Dr. Benjamin Smith	(Inria/École Polytechnique)	for the degree of
Prof. dr. Walter Van Assche	(KU Leuven)	Doctor of Science (PhD):
Prof. dr. ir. Frederik Vercauteren	(KU Leuven)	Mathematics

February 28, 2024

Contents

Preface	ix
1 Preliminaries	1
1.1 Elliptic Curves	1
1.1.1 Definition and Weierstrass models	1
1.1.2 Isogenies between elliptic curves	2
1.1.3 Elliptic curves over finite fields	3
1.2 Orientations and CM	4
1.2.1 Imaginary quadratic orders	4
1.2.2 Elliptic curves over \mathbf{C}	4
1.2.3 The CM method	5
1.2.4 Orientations	6
1.3 Bibliography	7
2 Isogeny-based cryptography	9
2.1 Diffie–Hellman key exchange	9
2.2 Class group action based key exchanges	11
2.2.1 Obtaining a key exchange from a class group action	11
2.2.2 Defining the class group action	12
2.2.3 Computing the class group action	13
2.2.4 OSIDH	15
2.3 SIDH	16
2.4 Bibliography	17
3 Main Results	19
3.1 Pairing-based attacks on class group action based cryptography	19
3.1.1 Self-pairings	19
3.1.2 Isogeny interpolation	20
3.1.3 Main contributions	21
3.2 Generalized class polynomials	24
3.2.1 Class polynomials	24
3.2.2 Main contributions	26
3.3 Radical isogenies	30

Contents

3.3.1	Computing isogeny chains	30
3.3.2	Main contributions	32
3.4	Bibliography	34
4	On the DDH problem for class group actions	37
4.1	Introduction	39
4.2	Background	42
4.2.1	Assigned characters	42
4.2.2	Class group action	43
4.3	Evaluating characters using the Weil pairing	44
4.3.1	Preliminaries	44
4.3.2	Evaluating the characters χ_m	45
4.3.3	Evaluating δ , ϵ or $\delta\epsilon$	45
4.4	Complexity and consequences for DDH	49
4.5	Reductions to endomorphism ring computation	52
4.5.1	The supersingular endomorphism ring problem	53
4.5.2	Action inversion problems	53
4.5.3	Action inversion reduces to endomorphism ring	54
4.6	Bibliography	58
5	Weak instances of class group action based cryptography via self-pairings	61
5.1	Introduction	63
5.2	Background	65
5.2.1	Oriented elliptic curves	65
5.2.2	Class group actions	67
5.2.3	Horizontal, ascending and descending isogenies	68
5.3	Generalized Weil and Tate pairings	68
5.3.1	Weil pairing	69
5.3.2	Tate pairing	70
5.4	Self-pairings	73
5.5	Constructing non-trivial self-pairings	78
5.5.1	A generalization of the ψ -Tate pairing	78
5.5.2	Self-pairings from divisors of the discriminant	79
5.5.3	Computing the self-pairings	80
5.6	Applications	82
5.6.1	Easy instances of class group action inversion	83
5.6.2	Decisional Diffie–Hellman revisited	89
5.7	Conclusions and open problems	91
5.8	Relaxing the compatibility assumption	92
5.9	Bibliography	97

6 Generalized class polynomials	101
6.1 Introduction	103
6.2 Generalized class polynomials	103
6.3 Estimates and reduction factors	106
6.3.1 Reduction factors	106
6.3.2 Measures of polynomials and heights of their roots	107
6.3.3 Proof of the height reduction	108
6.4 Class invariants for $X^0(N)$ and $X_+^0(N)$	111
6.4.1 Class invariants for $X^0(N)$	112
6.4.2 Real class polynomials from ramification	112
6.4.3 Real class polynomials from $X_+^0(N)$	113
6.4.4 Lower-degree class polynomials from ramification	115
6.4.5 Numerical results for $X_+^0(119)$	116
6.4.6 Comparison with existing class invariants	118
6.4.7 More modular curves of genus one	119
6.5 Application: the CM method	121
6.6 The computational benefits of our invariants	124
6.6.1 Space complexity of the functions	124
6.6.2 Speed of complex analytic computation	124
6.6.3 Adapting the CRT method	126
6.7 General curves and bases	128
6.8 Bibliography	132
7 Horizontal racewalking using radical isogenies	135
7.1 Introduction	137
7.2 Background	139
7.2.1 Division polynomials	139
7.2.2 Tate's normal form	140
7.2.3 Radical isogenies	140
7.3 Modular curves and Galois theory	142
7.3.1 Congruence subgroups	143
7.3.2 The main suspects	144
7.3.3 The Galois structure	144
7.4 Radical isogeny formulae through interpolation	146
7.4.1 A linear system	146
7.4.2 Finding the formulae	148
7.4.3 Iterative formulae	150
7.5 Optimizing the formulae	150
7.6 Ensuring horizontality	152
7.6.1 Horizontal vs. non-horizontal N -isogenies	153
7.6.2 Square vs. non-square radicands	155
7.6.3 Conjectural shape of ρ'_N modulo squares (proved for $N \leq 14$)	156
7.6.4 Horizontal isogenies and principal N th roots	157
7.7 Implementation	158
7.7.1 Isogeny chains	158

7.7.2	Impact on CSIDH	160
7.8	Bibliography	166
8	Conclusion	169
Samenvatting		171
Summary		175
Curriculum Vitae		179
List of Publications		181

Preface

Elliptic curves are mathematical objects that boast rich and deep connections to numerous areas of mathematics; most prominently to number theory and arithmetic geometry. They lie at the basis of many both solved and unsolved mathematical problems, such as Fermat’s last theorem and the Birch and Swinnerton-Dyer conjecture. In the real world, elliptic curves have become the standard in many cryptographic protocols, and they are used millions of times per second to establish encrypted communication over the internet. The security of these protocols relies on the assumption that a certain computational problem, called the *discrete logarithm problem*, is difficult. Quantum computers break this assumption, and hence much of today’s widely employed cryptography is considered potentially unsafe in the near future. An alternative proposal using elliptic curves is *isogeny-based cryptography*. It bases its security on the computational difficulty of finding a non-trivial map, also called an *isogeny*, between a pair of elliptic curves over a large finite field; a problem considered difficult even for quantum computers.

In Chapter 1, we present background material, consisting mainly of standard definitions and results related to elliptic curves and imaginary quadratic orders.

Chapter 2 provides a short introduction to isogeny-based cryptography, in particular to protocols that are based on class group actions.

In Chapter 3, we provide a summary of the ideas and main results of the following four chapters, all of which are papers jointly written with other authors.

Chapter 4 is a paper written together with Wouter Castryck, Frederik Vercauteren, and Benjamin Wesolowski. We analyze situations in which certain maps on elliptic curves called *pairings* can be used to break a computational hardness assumption called the *decisional Diffie–Hellman problem*.

Chapter 5 is a paper written together with Sam van Buuren, Wouter Castryck, Simon-Philipp Merz, Marzio Mula, and Frederik Vercauteren. We analyze special cases in which pairings can be used to recover a secret isogeny between a pair of elliptic curves over a large finite field.

Chapter 6 is a paper written together with Marco Streng. Motivated by a method to speed up the computation of elliptic curves over finite fields with a prescribed number of points, we devise a multivariate generalization of *Hilbert class polynomials*.

Chapter 7 is a paper written together with Wouter Castryck, Thomas Decru, and Frederik Vercauteren. It concerns a method to make isogeny-based protocols more practical by optimizing the underlying algorithms through *radical isogenies*.

In Chapter 8, we conclude by summarizing the main results and implications of our work. We also highlight some topics of further research.

We thank the Research Foundation – Flanders (FWO) for their support through PhD Fellowship Fundamental Research 11C7322N.

