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

Houben, M.R.

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. Derks	
	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)
Prof. dr. Ronald van Luijk	(Universiteit Leiden)
Dr. Chloe Martindale	(University of Bristol)
Dr. Benjamin Smith	(Inria/École Polytechnique)
Prof. dr. Walter Van Assche	(KU Leuven)
Prof. dr. ir. Frederik Vercauteren	(KU Leuven)

Dissertation presented in partial fulfillment of the requirements for the degree of Doctor of Science (PhD): Mathematics

February 28, 2024

Contents

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.