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

Houben, M.R.

Chapter 8

Conclusion

The main part of this work, Chapters 4, 5, 6, and 7, consists of four jointly written research papers.

In Chapter 4, we described a novel way in which pairings on elliptic curves can be used to attack the Decisional Diffie–Hellman problem for class group actions on oriented elliptic curves. We showed how the assigned character values associated to connecting ideal classes can be evaluated using the Weil pairing. This was previously only established for the Tate pairing. Our approach works more generally, is conceptually simpler, and speeds up the previous approach in certain cases. The attack only applies in case the class number is even. As a consequence, we recommend to restrict CSIDH and CRS to class groups of odd order.

In Chapter 5, we classified when non-trivial self-pairings on cyclic subgroups compatible with isogenies oriented by an imaginary quadratic order exist. Combining such self-pairings together with isogeny interpolation leads to a new attack strategy against CRS in the case where the degree of the secret isogeny is known. As a result of our classification, this implies the existence of weak instances of CRS; ones in which the discriminant has a large square smooth divisor coprime to the field characteristic.[1] One way to surely mitigate these attacks, is to use a discriminant of the form $-p$ where p is prime. CSIDH, in which the discriminant is of the form $-4p$, also remains unaffected by the strategy. An interesting future question to explore is whether small divisors of the discriminant could be exploited to obtain partial information about the secret isogeny. Furthermore, for some non-trivial self-pairings, we do not yet have an efficient algorithm to compute them; an interesting further topic of research would be to study the existence of efficient Miller-type algorithms for generalized Weil and Tate pairings. It would also be compelling to study whether the results of Chapters 4 and 5 can be unified and extended into a classification of self-pairings on general, not necessarily cyclic, subgroups compatible with oriented isogenies.

In Chapter 6, we devised generalized class polynomials; a multivariate extension of class polynomials. Class polynomials have previously been studied as a generalization of Hilbert class polynomials. The sizes of their coefficients are sometimes smaller by an asymptotic factor, improving their computational applicability in, for example, the CM method. The best known class polynomials obtain an asymptotic size reduction factor of 72. We showed that generalized class polynomials obtain provable asymptotic

[1] At the time of writing, upcoming work has been announced claiming that the condition that the divisor be *square* may be removed.

size reductions that were previously unattainable for a positive proportion of imaginary quadratic discriminants. However, our best such examples still have a reduction factor of at most 72. An interesting further research goal would be to find the first example of a family of generalized class polynomials, say of prime class number, that attain provable asymptotic size reductions beyond 72, or perhaps even exceeding the theoretical univariate bound of 100.83. Another goal is to extend the state-of-the-art method for computing class polynomials, a CRT-based approach by Sutherland, to the case of generalized class polynomials.

In Chapter 7, we studied radical isogenies; a method to compute chains of isogenies of fixed degree based on formulae containing a radical expression. We developed a new way to compute radical isogeny formulae that combines the CM method and Galois theory of function fields of modular curves with CRT-based rational interpolation. This extended the range of degrees in which formulae are available from $N \leq 13$ to all prime $N \leq 41$. Moreover, we simplified formulae and improved their computational performance. We also formulated a conjecture that states, in case of CSIDH, which radical must be taken for the corresponding radical isogeny to be horizontal, and proved this conjecture for all $N \leq 14$. A further goal would be to prove this conjecture for all (even) $N \geq 4$. It would also be interesting to find a method for producing general radical isogeny formulae that is more direct than by means of rational interpolation, for example by obtaining a closed form expression, or a linear recurrence relation satisfied by the formulae.