

Publication List

1. *Global divisibility of Heegner points and Tamagawa numbers*, to appear in *Compositio Mathematica*

Abstract. We improve Kolyvagin's upper bound on the order of the p -primary part of the Shafarevich–Tate group of an elliptic curve of rank one over a quadratic imaginary field. In many cases, our bound is precisely the one predicted by the Birch and Swinnerton-Dyer conjectural formula.

2. *Visibility of the Shafarevich–Tate groups at higher level*, with W. Stein, to appear in *Documenta Mathematica*

Abstract. We study visibility of Shafarevich–Tate groups of modular abelian varieties in Jacobians of modular curves of higher level. We prove a theorem about the existence of visible elements at a specific higher level under certain hypothesis which can be verified explicitly. We also provide a table of examples of visible subgroups at higher level and state conjectures inspired by our data.

3. *Explicit Heegner points: Kolyvagin's conjecture and non-trivial elements in the Shafarevich–Tate group*, with K. Lauter and W. Stein, to appear in *Journal of Number Theory*

Abstract. Kolyvagin used Heegner points to associate a system of cohomology classes to an elliptic curve over \mathbf{Q} and conjectured that the system contains a non-trivial class. His conjecture has profound implications on the structure of Selmer groups. We provide new computational and theoretical evidence for Kolyvagin's conjecture. More precisely, we explicitly compute Heegner points over ring class fields and use these points to verify the conjecture for specific elliptic curves of rank two. We explain how Kolyvagin's conjecture implies that if the analytic rank of an elliptic curve is at least two then the \mathbf{Z}_p -corank of the corresponding Selmer group is at least two as well. We also use explicitly computed Heegner points to produce non-trivial classes in the Shafarevich–Tate group.

4. *On the Computation of the Cassels Pairing for Certain Kolyvagin Classes in the Shafarevich–Tate Group*, with K. Eisentraeger and K. Lauter, submitted

Abstract. Kolyvagin has shown how to study the Shafarevich–Tate group of elliptic curves over imaginary quadratic fields via Kolyvagin classes constructed from Heegner points. In order to produce explicit nontrivial elements of the Shafarevich–Tate group, one has to be able to determine if a locally trivial Kolyvagin class is globally nontrivial, which is difficult in practice. We provide a method for testing whether an explicit element of the Shafarevich–Tate group represented by a Kolyvagin class is globally nontrivial by computing the Cassels pairing between certain locally trivial Kolyvagin cohomology classes. The algorithm uses the Tate cryptographic pairing which is efficiently computable and existing algorithms for explicit computation of Heegner points.

5. *On the Bits of Elliptic Curve Diffie–Hellman Keys*, with D. Jao and R. Venkatesan, *INDOCRYPT 2007*

Abstract. We study the security of elliptic curve Diffie–Hellman secret keys in the presence of oracles that provide partial information on the value of the key. Unlike the corresponding problem for finite fields, little is known about this problem, and in the case of elliptic curves the difficulty of representing large point multiplications in an algebraic manner leads to new obstacles that are not present in the case of finite fields. To circumvent this obstruction, we introduce a small multiplier version of the hidden number problem, and we use its properties to analyze the security of certain Diffie–Hellman bits. We suggest new character sum conjectures that guarantee the uniqueness of solutions to the hidden number problem, and provide some evidence in support of the conjectures by showing that the ones we need hold on average. We also present a Gröbner basis algorithm for solving the hidden number problem and recovering the Diffie–Hellman secret key when the elliptic curve is defined over a constant degree extension field and the oracle is a coordinate function in the polynomial basis.

6. *Random self-reducibility and bit security of the elliptic curve Diffie–Hellman secret keys*, with R. Venkatesan, submitted to *EUROCRYPT 2008*

Abstract. We prove that if one can predict the least significant bit of the Diffie–Hellman secret keys for elliptic curves with non-negligible advantage on a polynomial fraction of all curves over a given finite field \mathbf{F}_p , then one can compute the entire Diffie–Hellman secret on a polynomial fraction of all curves over the same finite field. Our method combines rapid mixing properties of certain isogeny graphs, results due to Boneh and Shparlinski and a new refinement of H. Lenstra’s lower bounds on the size of an isogeny classes corresponding to almost all traces of the Frobenius.