Pairing Friendly Elliptic Curves and Finite Fields

Igor E. Shparlinski, Macquarie University

We present some theoretic and heuristic estimates for the number of elliptic curves with low embedding which is essential for their applicability in pairing based cryptography. We also give estimates for the number of fields over which such curves may exist. The main ideas behind the proofs will be explained as well. Finally, we give a heuristic analysis of the so-called MNT algorithm and show that it produces a rather "thin" sequence of curves.