Abstract

We demonstrate that some finite fields, including $\mathbb{F}_{2^{210}}$, are weak for elliptic curve cryptography in the sense that any instance of the elliptic curve discrete logarithm problem for *any* elliptic curve over these fields can be solved in significantly less time than it takes Pollard's rho method to solve the hardest instances. We discuss the implications of our observations to elliptic curve cryptography, and list some open problems.