CORR 2001-59

Analysis of the GHS Weil Descent Attack on the ECDLP over Characteristic Two Finite Fields of Composite Degree

Markus Maurer*, Alfred Menezes & Edlyn Teske

Abstract In this paper, we analyze the Gaudry-Hess-Smart (GHS) Weil descent attack on the elliptic curve discrete logarithm problem (ECDLP) for elliptic curves defined over characteristic two finite fields of composite extension degree. For each such field $\mathbb{F}_{2^N}, N \in [100, 600]$, we identify elliptic curve parameters such that (i) there should exist a cryptographically interesting elliptic curve E over $\mathbb{F}_{2^N}$ with these parameters; and (ii) the GHS attack is more efficient for solving the ECDLP in $E(\mathbb{F}_{2^N})$ than for solving the ECDLP on any other cryptographically interesting elliptic curve over $\mathbb{F}_{2^N}$. We examine the feasibility of the GHS attack on the specific elliptic curves over $\mathbb{F}_{2^{176}}, \mathbb{F}_{2^{208}}, \mathbb{F}_{2^{272}}, \mathbb{F}_{2^{368}}$ that are provided as examples in the ANSI X9.62 standard for the elliptic curve signature scheme ECDSA. Finally, we provide several concrete instances of the ECDLP over $\mathbb{F}_{2^N}, N$ composite, of increasing difficulty which resist all previously known attacks but which are within reach of the GHS attack.