

**CORR 2001-26**

**Isomorphism Classes of Genus-2 Hyperelliptic Curves  
Over Finite Fields**

**L. Hernández Encinas\*, Alfred J. Menezes, & J. Muñoz Masqué**

**Abstract** We propose a reduced equation for hyperelliptic curves of genus 2 over finite fields  $\mathbb{F}_q$  of  $q$  elements with characteristic different from 2 and 5. We determine the number of isomorphism classes of genus-2 hyperelliptic curves having an  $\mathbb{F}_q$ -rational Weierstrass point. these results have applications to hyperelliptic curve cryptography.