Simple geometrically split abelian surfaces over finite fields

Kuo-Ming James Chou and Ernst Kani

Abstract: In this paper we study simple abelian surfaces A over a finite field $\mathbb{F}_q$ which are not simple (i.e., which are split) over the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$. After presenting a *classification theorem* of such surfaces, we discuss various *existence theorems* for these surfaces. Some of these results are closely linked to the structure of the *Weil restrictions* of certain elliptic curves $E/\mathbb{F}_{q^n}$, as is explained in Section 4.

In the last section we apply our results to the study of the Jacobians $J_{u,v}$ of a family of genus 2 curves $C_{u,v}$ which were first studied by Legendre in 1832 and more recently by Satoh in 2009 in connection with Public Key Cryptography. As a result, we can refine and simplify Satoh's method for constructing cryptographically safe genus 2 curves.