Point counting in genus 2: towards 128 bits

Pierrick Gaudry[a], Nicole Pitcher[b], and Éric Schost[c]

[a]Cacao project, LORIA, France

[b]Department of Mathematics, Statistics, and Computer Science, the University of Illinois at Chicago, IL, USA

[c]Department of Computer Science, the University of Western Ontario, Canada

Recent work on efficient group operations shows that genus 2 cryptosystems can be competitive with, or faster than, their elliptic analogues, for a similar level of security. One of the last missing steps is the determination of a suitable, secure curve over a prime field of size about 2^{128}.

I will describe ongoing work towards this goal, and review some of the underlying algorithms, from factorization in high degree extensions to lifting techniques for triangular sets.