EYAL GOREN, McGill University

The computational complexity of generating genus 2 curves suitable for cryptography

In his 2010 Leiden Thesis, M. Streng had determined the computational complexity of generating genus 2 curves suitable for cryptography. I will quickly recall a method of generating such curves and talk about one of the key elements in Streng's analysis, which is a recent theorem of K. Lauter (Microsoft Research) and myself.