DENIS CHARLES, Microsoft Research

Some applications of the graph of supersingular elliptic curves over a finite field

The graph of supersingular elliptic curves over a finite field connected by isogenies has many applications in computational number theory. In this talk we look at some old (in number theory) and new (in cryptography) applications of these graphs. In particular, we discuss new constructions of secure hash functions and pseudorandom number generators from these graphs.