

1018-11-189

Denis Charles* (cdx@microsoft.com), One Microsoft Way, Redmond, WA 98052, and **Eyal Goren** and **Kristin Lauter**. *Some applications of the graph of supersingular elliptic curves.*

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 applications (in cryptography) of these graphs. In particular, we discuss new constructions of secure hash functions and pseudorandom number generators from these graphs. (Received March 06, 2006)