Twisted Edwards Curves Tutorial

Emilie Menard Barnard
emilie@cs.ucsb.edu

November 1, 2015

Abstract

Edwards curves are a family of elliptic curves often used for cryptographic schemes. They exist over finite fields and, while they are practically used in security measures, they are often studied for their mathematical properties.

Twisted Edwards curves are a generalization of the more popular Edwards curves. These generalized curves are used in important security schemes as well, and thus are also worth studying.

My project will be a tutorial of Twisted Edwards curves. I plan to introduce them in comparison to Edwards curves, and review standard group law operations. I will compare and contrast Twisted Edwards curves and Edwards curves, and present which scenarios work best for which form. I will also briefly introduce an extended coordinate system on which one can consider inverted and projective Twisted Edwards curves. Lastly, I will present the latest research regarding Twisted Edwards curves and their applications.

References

Bernstein, Daniel J., Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. "Twisted Edwards Curves."Cryptology EPrint Archive (2008): Web. `http://eprint.iacr.org/2008/013.pdf`.

Edwards, Harold M. "A Normal Form for Elliptic Curves." American Mathematical Society 44.3 (2007): 393-422. Web. `http://www.ams.org/journals/bull/2007-44-03/S0273-0979-07-01153-6/S0273-0979-07-01153-6.pdf`.

Wroski, Micha. "Faster Point Scalar Multiplication on NIST Elliptic Curves over GF(p) Using (twisted) Edwards Curves over GF(p3)." Cryptology EPrint Archive (2015): Web. `http://eprint.iacr.org/2015/977.pdf`.