Binary Edwards Curves in Elliptic Curve Cryptography

Graham Enos

Preprint no. 2013-06

Abstract

Edwards curves are a new normal form for elliptic curves that exhibit some cryptographically desirable properties and advantages over the typical Weierstrass form. Because the group law on an Edwards curve (normal, twisted, or binary) is complete and unified, implementations can be safer from side channel or exceptional procedure attacks. The different types of Edwards provide a better platform for cryptographic primitives, since they have more security built into them from the mathematic foundation up.

Of the three types of Edwards curves – original, twisted, and binary – there hasn't been as much work done on binary curves. We provide the necessary motivation and background, and then delve into the theory of binary Edwards curves. Next, we examine practical considerations that separate binary Edwards curves from other recently proposed normal forms. After that, we provide some of the theory for binary curves that has been worked on for other types already: pairing computations. We next explore some applications of elliptic curve and pairing-based cryptography wherein the added security of binary Edwards curves may come in handy. Finally, we finish with a discussion of e2c2, a modern C++11 library we've developed for Edwards Elliptic Curve Cryptography.

Department of Mathematics, UNC Charlotte, Charlotte, NC 28223