Koblitz Curves and its practical uses in Bitcoin security

Kristian Bjoernsen
krbjorn@umail.ucsb.edu

1. November 2015

Abstract

Koblitz curves are a type of elliptic curves characterized by its non-random construction which allows for especially efficient computation. This is different from the most commonly used elliptic curves that have a pseudo-random structure where the parameters are chosen by a specified algorithm. With the rise of online cryptocurrency we are seeing practical uses and implementations of Koblitz curves in the exchange and ownership of cryptocurrency.

Bitcoin uses a specific Koblitz curve *secp256k1* defined by the Standards for Efficient Cryptography Group (SECG). The curve is defined over the finite field F_p :

$$y^2 = x^3 + ax + b$$

With a = 0, b = 7

In my project I plan to introduce Koblitz curves and look at its advantages or disadvantages in comparison to normal pseudo-random curves. I want to explore the different defined Koblitz curves from SECG and see why the specific curve *secp256k1* was chosen by the creator of Bitcoin. I also want to give an overview of how the Bitcoin protocol uses Koblitz curves to ensure security in signing and transferring funds.

References

[1] Standards for Efficient Cryptography *SEC 2: Recommended Elliptic Curve Domain Parameters* January 27, 2010 [http://www.secg.org/sec2-v2.pdf].

[2] Jerome A. Solinas *Efficient Arithmetic on Koblitz Curves* National Security Agency, Ft. Meade. March 2000.