A Study of Koblitz Curves

Tawny Lim *

November 1, 2015

Abstract

Koblitz curves are a type of elliptic curve that is defined over $\mathbb{F}_2$. These curves are advantageous in that they can be used to create point multiplication algorithms without the need for point doubling [1]. This paper aims to understand the uses of Koblitz curves in cryptography, including its advantages and disadvantages. We will begin by analyzing the properties of Koblitz curves. We will then look into the advantages of Koblitz curves, including speeding up scalar multiplication [2], and later examine some methods proposed by Solinas to further enhance the execution speeds of point multiples on Koblitz curves [4]. Afterwards, we will delve into a discussion concerning the current state of security regarding curves on binary fields and the possible risks of using Koblitz curves [3].

References

[1] Hankerson, Darrel, Menezes, Alfred, and Vanstone, Scott. *Guide to Elliptic Curve Cryptography.* New York: Springer, 2004.

[2] Koblitz, Neal. "Good and Bad Uses of Elliptic Curves in Cryptography." *Moscow Mathematical Journal* 2.4 (Oct.-Dec. 2002): 693-715.

[3] Koblitz, Neal, and Menezes, Alfred J. "A Riddle Wrapped in an Enigma." (2015).

[4] Solinas, Jerome A. "Efficient Arithmetic on Koblitz Curves" *Designs, Codes and Cryptography* 19 (2000): 195-249.

*Department of Computer Science, University of California, Santa Barbara, CA 93106. E-mail: tlim@cs.ucsb.edu