Pseudo Random Number Generation over Elliptic Curves

Josephine Vo
josephinevo@umail.ucsb.edu

December 1, 2015

1. Abstract

A deterministic random number generator (DRNG) can be implemented using the arithmetic defined for an elliptic curve group over a finite field. Arithmetic in the elliptic curve group depends on various parameters, so it yields points whose origins are difficult to assert. This makes it so our random number generator is seemingly unpredictable and ensures forward and backward security.

In this paper we will be investigating the fundamentals of algorithms which use elliptic curves to produce random values and their strengths. First we will describe the basics structure of the elliptic curve group. Next we will break down how we generate random numbers using such a curve step by step. We will also delve into the specifics of two types of curves that can be used and how they perform relative to one another: Edwards Curves and Weierstrass Curves. Lastly we will discuss the benefits of using elliptic curves over other methods.

References

1. koc-rng.pdf
2. 01DRNGECC-LS.pdf