1 Introduction

Randomness is crucial in cryptography, especially for key generation, which is usually the first step in any cryptographic protocol. Traditionally, there are two types of random number generators (RNGs): truly random number generators (TRNG) and Pseudorandom Number Generators (PRNG). A PRNG will receive a initial random seed of a given security level and produce seemingly randomness forever. A hybrid construction will incorporate true randomness into this process, allowing the RNG to accumulate entropy even if it is attacked by an adversary. However, special definition of security is needed in this case. Our first intuition for such a construction was to use established Elliptic Curve random number generators and “jump” between curves using outside randomness. However, further investigation into the structure of mappings between curves and the underlying security definitions of RNG showed that this might not be such a good idea. In addition, heuristic pingings between curves and the underlying security definitions of RNG to accumulate entropy were it to be attacked by an adversary.

2 Preliminaries

For the context of this paper, let \( K \) denote a finite field such that \( char(K) \neq 2 \). For \( n \in \mathbb{N} \), \([ n ]\) denotes the set \( \{1,..., n\} \) of integers from 1 to \( n \) and \( 0 \) otherwise. The projective 2-space over \( K \), \( \mathbb{P}^2(K) \), is defined to be \( \mathbb{P}^2(K) = \{(x,y,z) \mid \text{ with } x,y,z \in K, x,y,z \neq 0 \} \). Let \( S \) be an nonempty finite set, then \( \mathcal{B} \subseteq S \) means \( X \) is a random variable uniformly and independently sampled from \( S \). Let \( R \) be a random variable, then \( Y = R \) means \( Y \) is another random variable that is independent and identically distributed to \( Y \).

3 Elliptic Curves

Definition An elliptic curve is a pair \( (C,O) \), where \( C \) is a smooth projective curve (projective variety of dimension one) of genus one (see [5] for precise definitions), with one specified base point, \( O \).

With the excluded point, every elliptic curve has a natural group structure where the excluded point is the identity. [5-III-4]

3.1 Edwards Curves

A Twisted Edwards curve is given by the equation

\[
ax^2+y^2=1+dx^2y^2
\]

where \( a,d \in K \), with the base point \((1,0)\). An twisted Edwards curve over \( K \) is denoted \( E_{a,d}(K) \). For the special case \( a=1 \), we denote the curve \( E_{d}(K) \) and call it an Edwards curve.

Proposition 3.1. The binary operation, \( + \), defined on \( E_{a,d}(K) \) by

\[
(x_1,y_1) + (x_2,y_2) = \left( \frac{y_1 + y_2}{x_1 + x_2}, \frac{x_1 - x_2}{y_1 - y_2} \right)
\]

gives a group structure on \( E_{a,d}(K) \) with \((0,1)\) as the identity element.

3.2 Maps Between Curves

In order to “jump” between curves, we need some structural preserving and easy to compute maps between them. This section introduces rational maps and morphisms, which are equivalent on elliptic curves.

Definition Given two (projective) curves \( C,D \). A rational map (defined over \( K \)), \( \phi : C \rightarrow D \), is a map that can be written as fractions of homogeneous polynomials (over \( K \)), \( \phi = \phi_1 : \frac{f_1}{f_2} \) where \( f_1 \) and \( f_2 \) are homogeneous in \( x,y \in K \).

Definition Let \((C,O),(D,O')\) be elliptic curves. A morphism \( \phi : C \rightarrow D \) such that \( \phi(O) = O' \) is called an isogeny.

Theorem 3.2. An isogeny \( \phi : C \rightarrow C' \) defines a group homomorphism \( \phi \) on the corresponding group structure of \( C \) and \( D \).

Theorem 3.3. Let \( \phi : C \rightarrow C' \) be an isogeny, then the kernel of the group homomorphism, \( \ker(\phi) \), is finite.

Theorem 3.4. Let \( \phi : C \rightarrow D \) be a nonconstant isogeny of degree \( m \). There exists a unique isogeny, \( \phi : D \rightarrow C \), such that \( \phi \circ \phi = [m] \).

With the power of those theorems, it is easy to check that isogenies define an equivalent relation (and notice that the structure of this equivalence relation depends on the field \( K \) of definition). If there exists a non-trivial isogeny \( C \rightarrow D \), we say that \( C \) is isogenous to \( D \), which is denoted \( C \simeq D \).

Theorem 3.5. (Tate). Let \( K \) be a finite field, and \( C,D \) be elliptic curves. Then \( C \simeq D \) if and only if \( \phi(C) \neq \phi(D) \) and \( \phi(1) \neq 0 \).

Using the above machinery, Bernstein et al. [3] have shown that an elliptic curve (over a finite field) has an Edwards form if and only if the order of the group is divisible by 4.

Theorem 3.6. Let \( E \) be any elliptic curve over \( K \), then \( \#E(K) = \#E(K) \) and \( \#E(K) \)

It is tempting to expand a cryptographic object from one elliptic curve to the other by isogenies and to map intensions of the isogeny to maps between curves. However, we will see that this is not possible and the underlying computational problem harder.

4 Computational Indistinguishability

The notion of semantic security is usually defined against attacking adversaries, which is usually modeled as probabilistic Turing machines, the (rough) definition of which is given below

Definition A probabilistic Turing machine is a standard Turing machine such that at each step, the set of possible transitions has a probability distribution, according to which the Turing machine will take the next transition.

The notion of computational indistinguishability is crucial in the definition of pseudorandomness.

Definition A function \( f : N \rightarrow \{0,1\}^n \) is negligible if for every positive polynomial \( p(n) \), exists \( N \in \mathbb{N} \) such that for all \( n \geq N \), \( \left| f(n) \right| \leq \frac{1}{n^{p(n)}} \).

Definition Two sequence of random variables, \( S_k \), for \( k \in N \), are said to be computationally indistinguishable and denoted as \( S_k \approx S_0 \), if

\[
\Pr[\text{One of the next } k \text{ transitions takes a specific direction}] = \Pr[\text{One of the next } k \text{ transitions takes another specific direction}] \approx \frac{1}{2}
\]

is negligible in \( n \) for all polynomially bounded probabilistic Turing machines \( A \).

5 The Decisional Diffie-Hellman Problem and a Pseudorandom Generator

Definition Decision Diffie-Hellman problem (DDH)

A sequence of cyclic groups, \( (G_n)_{n \in \mathbb{N}} \), where \( G_n \) is of-bit-length \( n \), satisfies the DDH condition if for a generator \( g \), of \( G_n \), and given \( g, g^a, g^b, \) for random integers \( a, b \in [G_n] \), for \( \text{computational indistinguishability from} \{ [1,1], [1,0] \text{or } [0,1] \} \).

The DDH condition expresses the average-case hardness of the DDH problem. But for cryptographic purposes, we need worst-case hardness.

Theorem 5.1. Let \( G = \{G_n \mid n \in \mathbb{N} \} \) be a sequence of groups of prime order, and let \( a, b, c \in G \cup [G_n] \). Assuming the DDH condition holds for \( G \), there exists a probabilistic polynomial time algorithm \( A \) that decides, with overwhelming probability whether \( a \cdot ab \cdot c \) is divisible by \( c \).

8 Acknowledgements

I would like to thank my research directors, Ömer Eğecioğlu and Çetin Kayar Koç, for their mentorship, as well as my generous donor, Mr. Jay Fomenov, for supporting Summer Undergraduate Research Fellowship.

References
