Edwards Curves and Hybrid Pseudorandom Number Generators

Wei Dai

Research Directors: Ömer Eğecioğlu and Çetin Kaya Koç

University of California, Santa Barbara

Contact Information:
Wei Dai
College of Creative Studies
Email: wdai@umail.ucsb.edu

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 (RNG), namely true 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 were it to be attacked by an adversary. However, special definition of security is needed in this case. Our first intuition for such an construction was to use establised Elliptic Curve random number generators and "jump" between curves using outside randomness. However, a 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 Hybrid constructions are already in use on popular operating systems such as iOS and Windows. And a formal construction and analysis was done by Dodis et al [2].

2 Preliminaries

For the context of this poster, let K denote a finite field such that $charK \neq 2$. For $n \in \mathbb{N}$, $[n]$ denotes the set $\{1, ..., n\}$. $\delta_{i,j}$ is the Kronecker delta function, defined to be 1 if $i = j$ and 0 otherwise. The projective 2-space over K, $P^2(K)$, is defined to be, $\mathbb{P}^2(K) = (K^3 - (0,0,0))/\sim$, where

$$(a, b, c) \sim (x, y, z) \iff \exists \lambda \neq 0 \in K : \lambda(a, b, c) = (x, y, z)$$

Let S be an non-empty finite set, then $X \xleftarrow{R} S$ means X is a random variable taking values uniformly random from S. Let R be a random variable, then $Y \leftarrow R$ means that Y is another random variable that is independent and identically distributed to Y. Furthermore, we assume that any two random variables declared using $\leftarrow$ are independent.

3 Elliptic Curves

Definition An elliptic curve is a pair (C, O_C), 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, denoted O_C.

With the extinguished point, every elliptic curve has a natural group structure under which the extinguished point is the identity ([5, III.3]).

3.1 Edwards Curves

A Twisted Edwards curve is given by the equation

$$ax^2 + y^2 = 1 + dx^2y^2 \tag{1}$$

, where $a, d, x, y \in K$, with the base point $(0, 1)$. 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*

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}\right)$$

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 easily to compute maps between them. This section introduces rational maps and morphism, which are equivalent on elliptic curves.

Definition Given two (projective) curves C, D. A rational map (defined over K), $\phi : C(K) \to D(K)$, is a map that can be written as fractions of homogeneous polynomials (over K). i.e. $\phi = [f_0, f_1, f_2]$, where $f_i = \frac{g_i}{h_i}$ and $g_i, h_i \in K[x, y, z]$.

Definition Let $(C, O_C), (D, O_D)$ be elliptic curves. A morphism $\phi : C \to D$ such that $\phi(O_C) = O_D$ is called an isogeny.

Theorem 3.2. *An isogeny, $\phi : C \to D$, defines a group homomorphism on the corresponding group structure of C and D.*

Theorem 3.3. *Let $\phi : C \to D$ be an isogeny, then the kernel of the group homomorphism, $Ker\phi$, is finite.*

Theorem 3.4. *Let $\phi : C \to D$ be a nonconstant isogeny of degree m. There exists a unique isogeny, $\hat{\phi} : D \to C$, such that $\hat{\phi} \circ \phi = [m]$, the multiplication by m isogeny.*

With the power of these 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 of definition for the morphisms). If there exists a nonzero isogeny $C \to D$, we say that C is isogeneous to D, which is denoted $C \sim D$.

Theorem 3.5. *(Tate) Let K be a finite field, and C, D be elliptic curves. Then $C \sim_K D$ if and only if $\#C(K) = \#D(K)$.*

Using the above machinery, Bernstein el al. ([1]) showed that an elliptic curve (over a finite field) has an Edwards form if and only if the order of it is divisible by 4.

Theorem 3.6. *Let E be any elliptic curve over K, then $4 \mid \#E(K) \iff E(K) \cong_K E_d(K)$.*

It is tempting to expand a cryptographic object from one elliptic curve to the set of isogeneous elliptic curves and use the isogeny to map between curves. However, we will see that this is does not make 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 $f : \mathbb{N} \to \mathbb{R}$ is negligible if for every positive polynomial $p(x)$, there exists $N \in \mathbb{N}$ such that for all $n > N$, $|f(n)| < \frac{1}{p(n)}$.

Definition Two sequence of random varaibles, S_n, K_n for $n \in \mathbb{N}$, are said to be computationally indistinguishable, and denoted as $S_n \approx K_n$, if

$$|P_{s \leftarrow S_n}(A(s) = 1) - P(A_{k \leftarrow K_n}(k) = 1)|$$

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, $\{G_n \mid n \in \mathbb{N}\}$, where G_n is of bit-length n, satisfies the DDH condition if for a generator g_n of G_n, and given g_n^a, g_n^b for random integers $a, b \xleftarrow{R} [|G_n|]$, g_n^{ab} is computationally indistinguishable from g_n^c for $c \xleftarrow{R} [|G|]$. Or more precisely, if

$$\{(g_n^a, g_n^b, g_n^{ab}) \mid a, b \xleftarrow{R} [|G_n|]\} \approx \{(g_n^a, g_n^b, g_n^c) \mid a, b, c \xleftarrow{R} [|G_n|]\}$$

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

Theorem 5.1. *Let $\mathbb{G} = \{G_n \mid n \in \mathbb{N}\}$ be a sequence of groups of prime order, and let $(g_n, a, b, c) \xleftarrow{R} G_n \times [|G_n|]^3$. Assuming the DDH condition holds for $\mathbb{G}$, there exists a probabilistic polynomial time algorithm A that decides, with overwhelming probability whether $c = ab$ given g^a, g^b, g^c. Or more precisely,*

$$1 - P(A(g^a, g^b, g^c) = \delta_{c,ab})$$

is negligible.

There is an easy construction of a input-doubling pseudorandom generator based on the above results.

Lemma 5.2. *Let $\mathbb{G} = \{G_n \mid n \in \mathbb{N}\}$ be a sequence of groups of prime order. Let $G_n \in \mathbb{G}$, g be an generator of G_n, $a \in [|G_n|]$ and $X \xleftarrow{R} [|G_n|]$. Then, $F_{G_n,g,a} : [|G_n|] \to G_n \times G_n$, defined by*

$$F_{G_n,g,a}(b) = (g^b, g^{ab})$$

is a length-doubling PRG, or equivalent speaking, $F_{G_n,g,a}(X) \approx G_n \times G_n$.

6 Hybrid Construction

Is jumping between elliptic curves a good way to construct a Hybrid PRNG? In the last section, we saw that we need prime order groups (or groups with large prime factors, since we can take a subgroup of such a prime factor) in order to apply the above theorem. And the hardness of DDH is directly based on the largest prime factor. Therefore, mapping between curves does not increase the hardness of the underlying computationally hard problem.

The difficulty in constructing a Hybrid PRNG is to accumulate entropy properly. Assume that we are given uniform entropy $I_1, ..., I_k$, we need a construction that accumulates entropy. Dodis et al gave a simple construction based on polynomial-based universal hash functions ([2]). Here we present a more efficient construction based on squaring (inspired by Square Hash ([3])). Given a PRG, $\mathbf{G} : \{\mathbf{0}, \mathbf{1}\}^{\mathbf{n}} \to \{\mathbf{0}, \mathbf{1}\}^{\mathbf{m}}$, $m > n$ (such as the one constructed from the previous section), consider a Hybrid PRNG, which is a set three algorithms, (setup, refresh, next), defined as follows:

- setup(): output $seed = (X, X') \xleftarrow{R} \{0, 1\}^{2n}$, set $S = 0^n$.
- $S' =$ refresh$(S, I) = S + (X + I)^2$, where S' is the new state.
- next(): $(S', R) = \mathbf{G}(\mathbf{S})$, where R is the output.

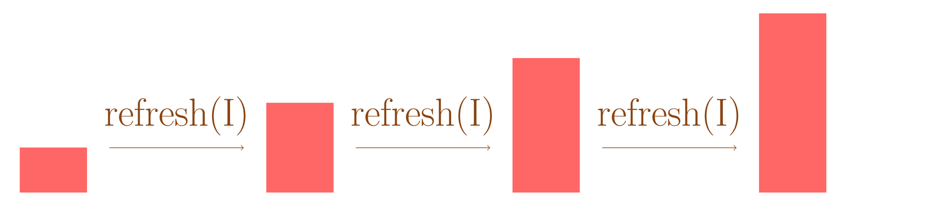

Figure 1: Entropy Accumulation in Hybrid PRNG

7 Furture Research

We saw that isogenies does not help with increasing the difficulty of the underlying computationally hard problem. What are the uses of isogenies in Cryptography? Can we utilize both the hardness of constructing isogenies and the DDH condition in a Cryptographic protocol?

8 Acknowledgements

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

References

[1] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. Twisted edwards curves. In *Proceedings of the Cryptology in Africa 1st International Conference on Progress in Cryptology*, AFRICACRYPT'08, pages 389–405, Berlin, Heidelberg, 2008. Springer-Verlag.

[2] Yevgeniy Dodis, Adi Shamir, Noah Stephens-Davidowitz, and Daniel Wichs. How to eat your entropy and have it too – optimal recovery strategies for compromised rngs. Cryptology ePrint Archive, Report 2014/167, 2014. http://eprint.iacr.org/.

[3] Mark Etzel, Sarvar Patel, and Zulfikar Ramzan. Square hash: Fast message authentication via optimized universal hash functions. In *In Proc. CRYPTO 99, Lecture Notes in Computer Science*, pages 234–251. Springer-Verlag, 1999.

[4] Moni Naor and Omer Reingold. Number-theoretic constructions of efficient pseudo-random functions. *J. ACM*, 51(2):231–262, March 2004.

[5] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2nd edition, 2009.