

# Constructing Pairing-Friendly Elliptic Curves

Peter Manohar, Xingyou Song

November 29, 2015

## Abstract

The goal of this report is to....

## Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Background</b>	<b>3</b>
<b>3</b>	<b>Constructing Pairing-Friendly Curves</b>	<b>6</b>
<b>4</b>	<b>Applications</b>	<b>7</b>

## 1 Introduction

### 1.1 Elliptic Curves

For our project, we shall define an elliptic curve to be a curve of the form:

$$E : y^2 = x^3 + Ax + B \tag{1}$$

where  $A$  and  $B$  are elements of some field  $\mathbb{F}$ , with  $\text{char}(\mathbb{F}) \neq 2, 3$ . The curve  $E$  is nonsingular if  $\frac{\partial F}{\partial x}$  and  $\frac{\partial F}{\partial y}$  are not simultaneously 0 for all points on  $E$ . It follows that  $E$  is nonsingular  $\iff x^3 + Ax + B$  has distinct roots. Through Vieta's formulas,  $E$  has distinct roots  $\iff ((r_1 - r_2)(r_1 - r_3)(r_2 - r_3))^2 = -(4A^3 + 27B^2)$  is nonzero. Therefore, we shall also require that the discriminant of  $E$ ,

$$\Delta = -16(4A^3 + 27B^2) \tag{2}$$

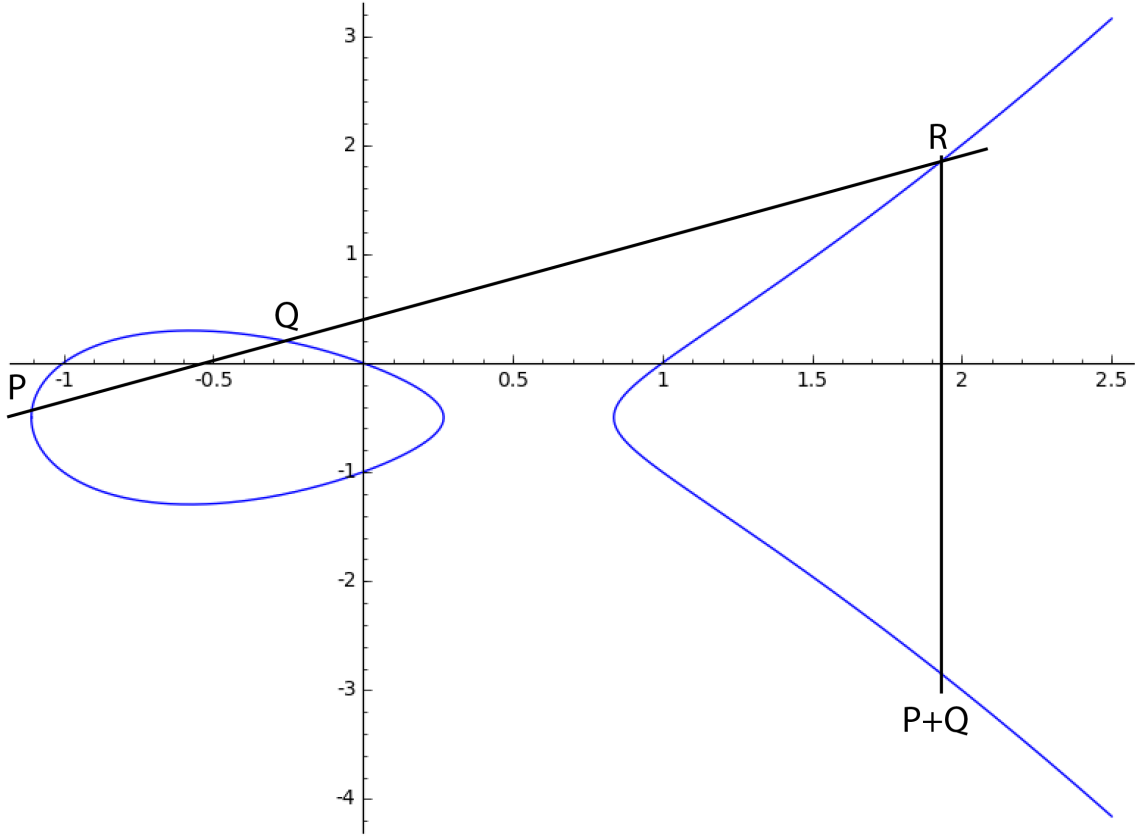
is nonzero. The j-invariant of  $E$  is defined by:

$$j(E) = 1728 \frac{4A^3}{4A^3 + 27B^2} \tag{3}$$

## 1.2 Group Law

The points on an elliptic curve form an additive abelian group. We shall define the group law geometrically.

Let  $P = (x_p, y_p)$ ,  $Q = (x_q, y_q)$ . A line through  $P$  and  $Q$  intersects  $E$  at a third point,  $R = (x_r, y_r)$ . We define  $P + Q := (x_r, -y_r)$ . Pictorially, this looks like



The group law can also be defined in terms of algebraic formulas, which can be found in [SIL08, III.2].

## 1.3 Notation

- $\mathbb{F}$  is a field
- $\overline{\mathbb{F}}$  is the algebraic closure of  $\mathbb{F}$
- $\mathbb{F}_p$  is a field with  $p$  elements, where  $p$  is prime
- $E(\mathbb{F}) = \{\mathbb{F} \times \mathbb{F} \mid E(x, y) = 0\}$
- $\phi$  is an isogeny (or endomorphism)
- $\phi_p$  is the Frobenius endomorphism
- $[n]$  is the multiplication by  $n$  map

## 2 Background

In this section, we shall define key concepts needed for our report. We will prove some of the more important results, and cite a source otherwise.

### 2.1 Isogenies

An isogeny of two elliptic curves  $E_1$  and  $E_2$  defined over a field  $\mathbb{F}$  is a nonconstant morphism  $\phi : E_1 \rightarrow E_2$ , where  $\phi$  is a group homomorphism from  $E_1(\overline{\mathbb{F}}) \rightarrow E_2(\overline{\mathbb{F}})$ .  $E_1$  and  $E_2$  are isomorphic if  $\exists \phi_1 : E_1 \rightarrow E_2$  and  $\phi_2 : E_2 \rightarrow E_1$ , isogenies, such that  $\phi_2 \circ \phi_1 = \text{Identity}$ .

#### 2.1.1 Separable and Inseparable Isogenies

Any isogeny  $\phi$  can be expressed as  $\phi(x, y) = (\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y)$ , where  $u, v, s, t \in \mathbb{F}[x]$ , and  $\gcd(u, v) = \gcd(s, t) = 1$ . An isogeny is separable if  $(\frac{u}{v})' \neq 0$ , and is inseparable otherwise. The degree of an isogeny is defined as  $\deg(\phi) := \max(\deg(u), \deg(v))$ . For any separable isogeny  $\phi$ ,  $\deg(\phi) = |\ker \phi|$ . [SUTH15]

#### 2.1.2 Dual isogenies

**Theorem 1** *Let  $\phi : E_1 \rightarrow E_2$  be an isogeny. Then  $\exists$  a unique  $\hat{\phi} : E_2 \rightarrow E_1$  such that  $\hat{\phi} \circ \phi = [n]$ , where  $n = \deg(\phi)$ .*

The proof of this can be found in either [SIL08] or [SUTH15]. Furthermore, for any two isogenies  $\phi_1$  and  $\phi_2$ ,  $\widehat{\phi_1 + \phi_2} = \hat{\phi}_1 + \hat{\phi}_2$ .

### 2.2 Endomorphisms

An endomorphism is an isogeny from  $E$  to itself. The endomorphisms of  $E$  form a ring, where addition is addition of functions and multiplication is function composition.

#### 2.2.1 Examples

The map  $[n] : E \rightarrow E$ , where  $[n]P = P + P + \dots + P$  ( $n$  times) is an endomorphism.

If  $E$  is defined over  $\mathbb{F}_p$ , the Frobenius map  $\phi_p : E \rightarrow E$  defined by  $\phi_p(x, y) := (x^p, y^p)$  is an (inseparable) endomorphism.

#### 2.2.2 Trace of an Endomorphism

**Theorem 2** *For any endomorphism  $\phi$ ,  $\phi + \hat{\phi} = 1 + \deg(\phi) - \deg(1 - \phi)$ , where we can regard the RHS as an endomorphism by the map  $n \mapsto [n]$ .*

**Proof:** As endomorphisms,

$$\begin{aligned} [\deg(1 - \phi)] &= \widehat{(1 - \phi)}(1 - \phi) = (\hat{1} - \hat{\phi})(1 - \phi) = (1 - \hat{\phi})(1 - \phi) \\ &= 1 - \hat{\phi} - \phi + \hat{\phi} \circ \phi = 1 - \hat{\phi} - \phi + [\deg(\phi)] \\ \implies \phi + \hat{\phi} &= 1 + [\deg(\phi)] - [\deg(1 - \phi)] \end{aligned}$$

□

By the above theorem, we can now define  $\text{trace}(\phi) := \phi + \hat{\phi}$ .

**Theorem 3**  $\#E(\mathbb{F}_p) = p + 1 - t$ , where  $t = \text{trace}(\phi_p)$

**Proof:** The fixed field of  $\phi_p$  is  $\mathbb{F}_p$ , and  $1 - \phi_p$  is separable (see [SUTH15]). Therefore,  $\ker(1 - \phi_p) = \#E(\mathbb{F}_p)$ . It is clear that  $\deg(\phi_p) = p$  by definition ( $u(x) = x^p$  and  $v(x) = 1$ ). We have that

$$\begin{aligned} \ker(1 - \phi_p) &= \deg(1 - \phi_p) = 1 + \deg(\phi_p) - \text{trace}(\phi_p) = p + 1 - t \\ \implies \#E(\mathbb{F}_p) &= p + 1 - t \end{aligned}$$

□

## 2.3 j-invariant

**Theorem 4** Two elliptic curves  $E_1(\mathbb{F})$  and  $E_2(\mathbb{F})$  are isomorphic over  $\overline{\mathbb{F}} \iff j(E_1) = j(E_2)$ . Furthermore,  $\forall j_0 \in \overline{\mathbb{F}}, \exists$  an elliptic curve  $E(\mathbb{F})$  such that  $j(E) = j_0$ .

The proof requires some lengthy algebraic manipulation, which can be found in [SIL08, III.1]. As a consequence of the proof, for any  $j \in \overline{\mathbb{F}}$ , we can define an canonical elliptic curve  $E$  associated with this j-invariant. We see that

$$\begin{aligned} E : y^2 &= x^3 + \frac{3j}{1728-j}x + \frac{2j}{1728-j} \text{ if } j \neq 0, 1728 \\ E : y^2 &= x^3 + 1 \text{ if } j = 0 \\ E : y^2 &= x^3 + x \text{ if } j = 1728 \end{aligned} \tag{4}$$

## 2.4 Twists

Two curves  $E_1(\mathbb{F})$  and  $E_2(\mathbb{F})$  are *twists* if they are isomorphic over  $\overline{\mathbb{F}}$  but not over  $\mathbb{F}$ .

### 2.4.1 Quadratic Twists

In particular, we are interested in quadratic twists. If  $E : y^2 = x^3 + Ax + B$  is an elliptic curve defined over  $\mathbb{F}$ , and  $d \in \mathbb{F}$  is a nonsquare, then we define the *quadratic twist* of  $E$  as  $\tilde{E} : y^2 = x^3 + d^2Ax + d^3B$ .

**Theorem 5** If  $E : y^2 = x^3 + Ax + B$  is an elliptic curve over  $\mathbb{F}_p$  with  $\#E(\mathbb{F}_p) = p + 1 - t$ , then  $\#\tilde{E}(\mathbb{F}_p) = p + 1 + t$

**Proof:** Let  $\left(\frac{\cdot}{p}\right)$  be the legendre symbol mod  $p$ . For any  $x \in \mathbb{F}_p$ , we see that  $1 + \left(\frac{x^3 + Ax + B}{p}\right) = \#$  of points on  $E$  with x-coordinate  $x$ . Therefore,

$$\#E(\mathbb{F}_p) = 1 + \sum_{x \in \mathbb{F}_p} \left(1 + \left(\frac{x^3 + Ax + B}{p}\right)\right) = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + Ax + B}{p}\right)$$

Since  $\mathbb{F}_p$  is a field,  $\forall x \in \mathbb{F}_p, \exists x' \in \mathbb{F}_p$  such that  $dx' = x$ . Therefore, for  $\tilde{E}(\mathbb{F}_p)$ , we have that

$$\begin{aligned} \#\tilde{E}(\mathbb{F}_p) &= 1 + \sum_{x \in \mathbb{F}_p} \left(1 + \left(\frac{(dx)^3 + A(dx) + B}{p}\right)\right) = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{d^3(x^3 + Ax + B)}{p}\right) \\ &= p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{d}{p}\right) \left(\frac{d^2}{p}\right) \left(\frac{x^3 + Ax + B}{p}\right) = p + 1 - \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + Ax + B}{p}\right) \end{aligned}$$

□

## 2.5 Pairings and Pairing-Friendly Curves

Let  $G$  be an additive abelian group of order  $p$ , a prime, and let  $G'$  be a multiplicative group of order  $p$ . A pairing is a bilinear map  $e : G \times G \rightarrow G'$  satisfying:

1. (bilinearity)  $e(P_1 + P_2, P_3) = e(P_1, P_3)e(P_2, P_3) \forall P_1, P_2, P_3 \in G$
2. (non-degeneracy)  $e(P, P) \neq 1$ , where  $G = \langle P \rangle$
3. (computability)  $e$  is efficiently computable

[PAIR91]

### 2.5.1 Weil and Tate Pairings

Let  $E[r] = \{P \in E(\mathbb{F}_p) \mid rP = O\}$  be the  $r$ -torsion group of  $E(\mathbb{F}_p)$ .

The Weil Pairing is a map  $e_r : E[r] \times E[r] \rightarrow \mu_r$ , where  $\mu_r$  is the set of  $r$ th roots of unity in  $\overline{\mathbb{F}_p}$ .

The Tate Pairing is a map:  $\tau_r : E(F_p)[r] \times E(F_p)[r]/rE(F_p) \rightarrow \mu_r$ , where  $\tau_r(P, Q) = e_r(P, R - \phi_p(R))$ , where  $R$  satisfies  $rR = Q$ . [WASH08]

### 2.5.2 Embedding Degree

We do not need the full algebraic closure  $\overline{\mathbb{F}_p}$  to determine  $\mu_r$ . Instead, we can find a positive integer  $k$  such that  $\mu_r \subset \mathbb{F}_{p^k}$ , that is, we require only a finite degree algebraic extension. We define the embedding degree  $k$  of  $E(\mathbb{F}_p)$  with respect to  $r$  as  $k := [\mathbb{F}_p(\mu_r) : \mathbb{F}_p]$ , the degree of the extension field. Therefore, we can regard  $k$  as the smallest positive integer such that  $\mu_r \subset \mathbb{F}_{p^k}$ .

Alternatively, suppose that  $k$  is the smallest positive integer such that  $\mu_r \subset \mathbb{F}_{p^k}$ .  $\mu_r \subset \mathbb{F}_{p^k} \iff r \mid \#\mathbb{F}_{p^k}^*$  (since multiplicative groups of finite fields are cyclic)  $\iff \gcd(r, p^k - 1) = r \iff p^k - 1 \equiv 0 \pmod{r} \iff p$  is a primitive  $k$ th root of unity mod  $r$  (since we picked  $k$  to be minimal).

Therefore, the embedding degree  $k$  is the smallest positive integer satisfying  $p^k \equiv 1 \pmod{r}$ .

### 2.5.3 Pairing-Friendly Curves

The Weil/Tate Pairing is efficiently computable when  $k$  is small, as computing the pairings requires computation in  $\mathbb{F}_{p^k}$ . A curve with efficiently computable pairings is *pairing-friendly*. Pairing-friendly curves are rare. In general, if  $r \approx p$ , then  $\Pr[\text{pairing-friendly curve}] = O(\frac{\log^3 M}{M})$ . [IM98]

## 3 Constructing Pairing-Friendly Curves

### 3.1 Complex Multiplication Method

**Input:**  $p$ , a prime, and  $N$  a positive integer  
**Output:** An elliptic curve  $E(\mathbb{F}_p)$  where  $\#E(\mathbb{F}_p) = N$   
 $t := p + 1 - N$ ;  
 $D = \text{square free part of } t^2 - 4p$ ;  
 $H_D(x) = \text{Hilbert class polynomial}$   
 Pick  $j \in \mathbb{F}_p$  such that  $H_D(j) = 0$  Compute  $E$  according to (4).  
**if**  $\#E(\mathbb{F}_p) = N$  **then**  
   | **return**  $E$   
**else**  
   | **return** quadratic twist of  $E$   
**end**

As a result from the theory of complex multiplication, the above algorithm will always succeed provided that such a curve  $E$  exists and will be efficient if  $D$  is not too large [SUTH15]. A slight subtlety arises if  $j = 0$  or  $j = 1728$ . If  $j = 0$ , then there are 6 classes of curves, corresponding to sextic twists of  $E$  by  $1, \zeta, \zeta^2, \dots, \zeta^5$ , for  $\zeta$ , a primitive root of unity in  $\mathbb{F}_p$ . If  $j = 1728$ , then there are 4 classes of curves, corresponding to quartic twists of  $E$  by  $1, \zeta, \dots, \zeta^3$ , for  $\zeta$ , a primitive root of unity in  $\mathbb{F}_p$ . If a curve  $E$  exists, then one of these curves will satisfy the conditions of the algorithm. [SIL08, III.10]

### 3.2 Cocks Pinch Method

We wish to construct a curve with a subgroup of size  $r$  and embedding degree  $k$ . Suppose we also have chosen a CM discriminant  $D$  such that  $(\frac{D}{r}) = 1$ . The Cocks Pinch method finds a prime  $p$  and the trace of Frobenius  $t$  such that  $\exists$  an elliptic curve  $E$  over  $\mathbb{F}_p$  with trace  $t$ , and a subgroup of size  $r$  with embedding degree  $k$ . There are 3 conditions on  $p, t$ :

1.  $t^2 - 4p = f^2 D$ , for some  $f$ . This means that  $E$  has CM discriminant  $D$
2.  $p + 1 - t \equiv 0 \pmod{r}$ . This means that  $r \mid \#E(\mathbb{F}_p) \implies$  there is a subgroup of size  $r$  by the characterization of finitely generated abelian groups
3.  $p$  is a primitive  $k$ th root of unity mod  $r$ . As mentioned earlier, this condition is equivalent to  $E$  having embedding degree  $k$  with respect to the subgroup of size  $r$ .

We see that we only need to satisfy the above 3 conditions for  $p, t$ . To do this, we first choose  $g$ , a primitive  $k$ th root of unity mod  $r$ . We know that  $t - 1 \equiv p \equiv g \pmod{r}$ . Using (1), we see that  $\frac{(t^2 - f^2 D)}{4} = p$ . We can set  $a = 2^{-1}(g + 1) \pmod{r}$  (as integers). Then,  $2a \equiv g + 1 \equiv t \pmod{r} \implies a^2 \equiv \frac{t^2}{4} \pmod{r}$ . We can also set  $f_0 = \frac{2(a-1)}{\sqrt{D}} \pmod{r}$ . Suppose  $p = \frac{(t^2 - f_0^2 D)}{4}$  is prime, and  $t = 2a$ . Then  $p + 1 - t \equiv a^2 - (a - 1)^2 + 1 - t \equiv 2a - 1 + 1 - t \equiv 0 \pmod{r}$ , so that (2) is satisfied, and (2)  $\implies$  (3) since  $t - 1 \equiv g$ . (1) is satisfied by construction of  $p$ , and so we have the desired output. If  $p$  is not prime, then we can compute  $p = \frac{(t^2 - f^2 D)}{4}$  for  $f = f_0 + ir$ , which gives new values for  $p$  while preserving the above congruences mod  $r$ . If the algorithm succeeds in finding a prime  $p$  then it outputs  $p, t$ , and will output  $\perp$  if it fails. The algorithm is given below in pseudocode:

**Input:**  $k$ , embedding degree,  $r$ , size of subgroup,  $D$ , CM discriminant with  $(\frac{D}{r}) = 1$   
**Output:**  $p$ , a prime, and  $t$  a trace of Frobenius  
 $a := 2^{-1}(g + 1) \pmod{r}$  (as integers)  
 $f = \frac{2(a-1)}{d}$  (as integers where  $d \equiv \sqrt{D} \pmod{r}$ )  
 $t := 2a$   
 $p = \frac{(t^2 - f^2 D)}{4}$   
**while**  $p$  is not prime **do**  
     $f = f + r$   
     $p = \frac{(t^2 - f^2 D)}{4}$   
    **if** running for too long **then**  
        **return**  $\perp$   
    **end**  
**end**  
**return**  $p, t$

If the algorithm succeeds, we can use the CM method to construct the desired elliptic curve  $E$ , provided that  $E$  exists. We see that  $\frac{t^2}{4} \leq \frac{t^2 - f^2 D}{4} = p^2 \implies t \leq 2\sqrt{p}$  since  $D < 0$ . As part of the proof of the CM method [SUTH15], a curve  $E$  with trace  $t$  exists if (1) is satisfied,  $t \leq 2\sqrt{p}$ , and  $t \not\equiv 0 \pmod{p}$ . The last equation is satisfied since  $t > 0$  and  $p > t$ . Therefore,  $E$  exists.

### 3.3 Dupont Enge Morain Method

## 4 Applications

### 4.1 Elliptic Curve Discrete Logarithm Problem

The Elliptic Curve Discrete Logarithm Problem (ECDLP) is formalized as follows: Given two points  $P, Q$ , find an integer  $k$  such that  $kP = Q$ .

Currently, the fastest known method for solving ECDLP is Pollard's  $\rho$  method, which runs in  $O(\sqrt{p})$  time.

#### 4.1.1 Pohlig-Hellman Method

Suppose  $N = \#E(\mathbb{F}_p)$ , and write  $N = \prod_i q_i^{e_i}$  as a product of primes. To determine  $k$ , all we need to do is find  $k \pmod{q_i^{e_i}}$  and then construct  $k$  using the Chinese Remainder

theorem. This is the main idea behind the Pohlig-Hellman Method, which is efficient provided that the prime factors of  $N$  are small. [WASH08]

#### 4.1.2 MOV attack

The Menezes-Okamoto-Vanstone (MOV) attack relies on using pairings to solve the ECDLP. The idea behind the attack is to map the DLP on  $E$  to the DLP in  $\mathbb{F}_{p^k}$ , where  $k$  is the embedding degree, and then use the index calculus method to solve the DLP in subexponential time. This attack is efficient provided that  $k$  is small. However, elliptic curves generally have large embedding degree with respect to any large subgroup, so this attack is only useful against pairing-friendly elliptic curves.

## References

- [SIL08] Joseph H. Silverman The Arithmetic of Elliptic Curves, 2008.
- [WASH08] Lawrence C. Washington Elliptic Curves, Number Theory and Cryptography, 2008.
- [CMS10] Nigel Smart. Advances in Elliptic Curve Cryptography, 2010.
- [CEC10] K. Rubin and A. Silverberg. Choosing the Correct Elliptic Curve in the CM Method, 2010.
- [TAX10] David Freeman, Michael Scott, and Edlyn Teske. A Taxonomy of Pairing-Friendly Elliptic Curves, 2010.
- [FR06] David Freeman. Methods for Constructing Pairing Friendly Elliptic Curves, 2006.
- [EM08] Koray Karabina and Edlyn Teske. On Prime-Order Elliptic Curves with Embedding Degrees  $k = 3, 4$ , and  $6$ , 2008.
- [PAIR91] Alfred Menezes. An Introduction to Pairing-Based Cryptography, 1991.
- [SUTH15] Andrew Sutherland. MIT: Math 18.783 Elliptic Curves, Lectures, 2015.
- [IM98] R. Balasubramanian, N. Koblitz. The Improbability That an Elliptic Curve Has Subexponential Discrete Log Problem under the Menezes-Okamoto-Vanstone Algorithm, 1998.