Constructing Pairing-Friendly Elliptic Curves

Peter Manohar, Xingyou Song

December 2, 2015

Abstract

This report covers some of the fundamental aspects of elliptic curve construction. Specifically, we will focus on the Cocks-Pinch and Dupont-Enge-Morain methods for curve construction. We start by giving an overview of important concepts about elliptic curves needed for understanding these two methods, and then we will state and explain the two algorithms. Finally, we explore some of the applications of elliptic curves to cryptography.

Contents

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 $\partial F/\partial x$ and $\partial F/\partial y$ 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,

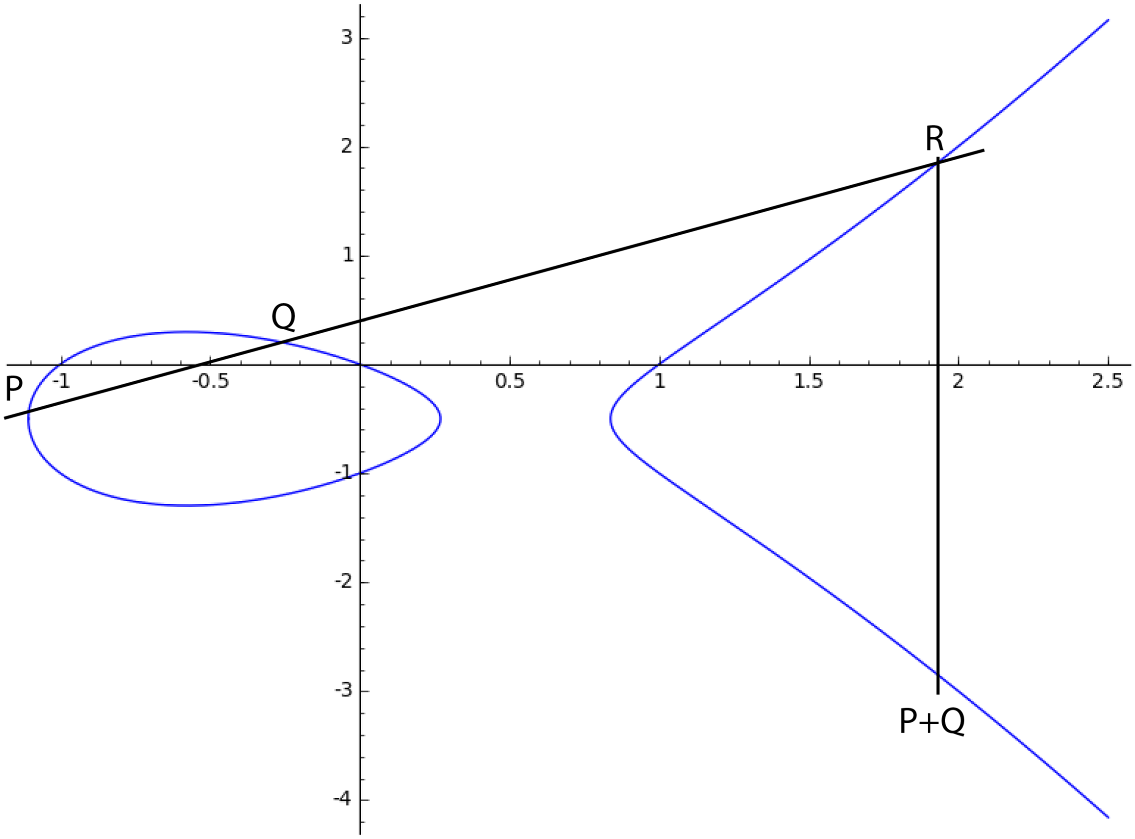
$$\Delta = -16(4A^3 + 27B^2) \tag{2}$$

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 $P + Q := (x_r, -y_r)$. Pictorally, 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
- $E(\mathbb{F}) = \{(x, y) \in \mathbb{F} \times \mathbb{F} \mid E(x, y) = 0\}$
- ϕ is an isogeny (or endomorphism)
- ϕ_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 $\phi : E_1 \to E_2$, where ϕ is a group homomorphism from $E_1(\overline{\mathbb{F}}) \to E_2(\overline{\mathbb{F}})$. E_1 and E_2 are isomorphic if there exist isogenies ϕ_1, ϕ_2 where $\phi_1 : E_1 \to E_2$ and $\phi_2 : E_2 \to E_1$ such that $\phi_2 \circ \phi_1 = \text{Identity}$.

2.1.1 Separable and Inseparable Isogenies

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

2.1.2 Dual isogenies

Theorem 1 *Let $\phi : E_1 \to E_2$ be an isogeny. Then $\exists$ a unique $\hat{\phi} : E_2 \to E_1$ 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 ϕ_1 and ϕ_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 $[n] : E \to E$, where $[n]P = P + P + \cdots + P$ (n times) is an endomorphism.

If E is defined over $\mathbb{F}_p$, the Frobenius map $\phi_p : E \to E$ 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 ϕ, $\phi + \hat{\phi} = 1 + \deg(\phi) - \deg(1 - \phi)$, 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 trace(ϕ) := $\phi + \hat{\phi}$.

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

Proof: The fixed field of ϕ_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 a canonical elliptic curve E associated with this j-invariant. We see that

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

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

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

$$= p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{d}{p} \right) \left(\frac{d^2}{p} \right) \left(\frac{x^3 + Ax + B}{p} \right) = p + 1 - \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + Ax + B}{p} \right)$$

□

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 $e : G \times G \to G'$ satisfying:

1. (bilinearity) $e(P_1 + P_2, P_3) = e(P_1, P_3)e(P_2, P_3)$ and $e(P_1, P_2 + P_3) = e(P_1, P_2)e(P_1, P_3)$ $\forall P_1, P_2, P_3 \in G$
2. (non-degeneracy) $e(P, P) \neq 1$, where $G = <P>$
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 $e_r : E[r] \times E[r] \to \mu_r$, where μ_r is the set of rth roots of unity in $\overline{\mathbb{F}_p}$.

The Tate Pairing is a map: $\tau_r : E(F_p)[r] \times E(F_p)[r]/rE(F_p) \to \mu_r$, 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 μ_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 $\mu_r \subset \mathbb{F}_{p^k}$. $\mu_r \subset \mathbb{F}_{p^k} \iff r \Big| \#\mathbb{F}^*_{p^k}$ (since multiplicative groups of finite fields are cyclic) $\iff p^k - 1 \equiv 0 \mod r \iff p$ is a primitive kth root of unity mod r (since we picked k to be minimal).

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

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[pairing-friendly curve] $= O(\frac{\log^3 p}{p})$. [IM98]

2.6 Ordinary Curves

Definition: $E(\mathbb{F}_p)$ is ordinary if $\#E[p] = p$. If $\#E[p] \neq p$ ($\#E[p] = 1$) then $E(\mathbb{F}_p)$ is supersingular.

For this project we are interested in constructing ordinary curves, as supersingular curves are vulnerable to attacks since they have embedding degree 2 over $\mathbb{F}_p$ for $p \geq 5$. We will see that the curve generation algorithms we use only construct ordinary curves.

2.7 Complex Multiplication

2.7.1 Complex Lattice

Theorem 6 *Let ω_1, ω_2 be linearly independent points in C. Define the lattice*

$$L = Z\omega_1 + Z\omega_2$$

Then there exists an elliptic curve that is isomorphic to $\mathbb{C}/L$.

Proof Sketch:

The Weierstrass $\wp(z)$ function is:

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in L} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right). \tag{5}$$

$\wp(z)$ is convergent, doubly periodic with periods ω_1 and ω_2, and is holomorphic on $\mathbb{C}$ everywhere except on L. The derivative of $\wp(z)$ is

$$\wp'(z) = -2 \sum_{\omega \in L} \frac{1}{(z-\omega)^2}. \tag{6}$$

$\wp(z)$ gives an isomorphism from $\mathbb{C}/L$ to $E(\mathbb{C})$, by the map

$$z \to (\wp(z), \wp'(z)), \quad 0 \to O$$

with E being defined as

$$E : y^2 = 4x^3 - g_2 x - g_3 \tag{7}$$

where $g_2 = 60G_4, g_3 = 140G_6$, and $G_k(L) = \sum_{\omega \in L} \omega^{-k}$ is the Eisenstein series of weight k.

It can be shown that addition of points on $E(\mathbb{C})$ corresponds to addition of points in $\mathbb{C}/L$. [SUTH15] Formally:

$$\big(\wp(z_1), \wp'(z_1)\big) + \big(\wp(z_2), \wp'(z_2)\big) = \big(\wp(z_1 + z_2), \wp'(z_1 + z_2)\big) \ . \tag{8}$$

We can also relate the j-invariant on curves to the j-function of a complex lattice. First, observe that we can rescale our lattice L to $Z\tau + Z$ where $\tau = w_1/w_2$, while preserving $\mathbb{C}/L$ as a group. The j-invariant of L is

$$j(\tau) = 1728 \frac{g_2^3}{g_2^3 - 27g_3^2} \ . \tag{9}$$

The theorem states that every lattice $\mathbb{C}/L \cong E(\mathbb{C})$ for some elliptic curve E. However, it turns out that the converse is also true. Namely, $E(\mathbb{C}) \cong \mathbb{C}/L$ for some lattice L. This establishes an isomorphism between the endomorphism rings of $E(\mathbb{C})$ and $\mathbb{C}/L$. The endomorphism ring of L is the set $\{\beta \in C | \beta L \subseteq L\}$. Therefore, we see that

$$End(E) \cong \{\beta \in \mathbb{C} | \beta L \subseteq L\} \tag{10}$$

where the endomorphism $[n]$ on E corresponds to $z \mapsto nz$ on L. Furthermore, there are endomorphisms in $End(E)$ that correspond to multiplication by multiplying the lattice by complex numbers. [WASH08]

For curves defined on a field $\mathbb{F}$, there is a homomorphism $\mathbb{F} \to C$ if we linearly map the finite basis elements of $\mathbb{F}$, $\alpha_1, ..., \alpha_n$ respectively to any algebraically independent set of elements in $\mathbb{C}$, $\tau_1, ..., \tau_n$, so we can regard $E(\mathbb{F})$ as a curve in $\mathbb{C}$.

2.7.2 Endomorphism Rings

Theorem 7 *The elements β in the endomorphism ring are algebraic integers that lie in some quadratic field $\mathbb{Q}[\sqrt{D}]$.*

Proof: Note that by theorem 6, there exist integers a, b, c, d such that

$$\begin{aligned} &\beta\omega_1 = a\omega_1 + b\omega_2 \quad \beta\omega_2 = c\omega_1 + d\omega_2 \\ &\implies \begin{bmatrix} \beta - a & -b \\ -c & \beta - d \end{bmatrix} \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix} = 0 \implies \det \begin{bmatrix} \beta - a & -b \\ -c & \beta - d \end{bmatrix} = 0 \\ &\implies \beta^2 - \beta(a + d) + (ad - bc) = 0 \end{aligned}$$

so β is an algebraic integer in a quadratic field $\mathbb{Q}[\sqrt{D}]$ as it is the root of a polynomial with coefficients in $\mathbb{Z}$. □

Definition: An *order* in an imaginary quadratic field is a ring R that is contained in the field.

It turns out that R will have have the form $\mathbb{Z}[f\frac{1+\sqrt{D}}{2}]$ if $D \equiv 1 \mod 4$ and $\mathbb{Z}[f\sqrt{D}]$ if $D \equiv 2, 3 \mod 4$, where D is a squarefree integer.
The endomorphism ring $End(E)$ is isomorphic to an order in a quadratic imaginary field [WASH08]. The discriminant of $End(E)$ is f^2D if $D \equiv 1 \mod 4$ and $f^2\,4D$ if

$D \equiv 2, 3 \mod 4$.

We state one final result that we will find useful.

Theorem 8 *Let E be an elliptic curve over $\mathbb{Q}$ with $End(E) \cong$ an order in $\mathbb{Q}[\sqrt{D}]$. Let p be a prime such that $p \not| \Delta(E)$. The following are equivalent:*

1. *$E(\mathbb{F}_p)$ is ordinary*
2. *$\left(\frac{D}{p}\right) = 1$ and $H_D(X)$ splits in $\mathbb{F}_p[x]$*
3. *$t^2 - 4p = f^2 D$, $t \not\equiv 0 \mod p$, for some integers t and f*

[WASH08], [SUTH15].

3 Constructing Pairing-Friendly Curves

3.1 Complex Multiplication Method

The Complex Multiplication (CM) method is an algorithm for constructing ordinary elliptic curves over $\mathbb{F}_p$ with N points. To do this, we set $t = p + 1 - N$, and let D be the square-free part of $t^2 - 4p$. Assuming $t \not\equiv 0 \mod p$, $H_D(x)$ will split completely in $\mathbb{F}_p[x]$, since $D \equiv t^2 \mod p$. Therefore, we can pick a root j_0 to be the j-invariant of the curve. We can then use the canonical representative of an elliptic curve with j-invariant j_0 to construct a curve E. The curve we construct could either have $N = p + 1 - t$ or $N = p + 1 + t$, since the sign of t does not matter when computing D. If $N = p + 1 - t$, then the quadratic twist of the curve will have $N = p + 1 - t$, as desired. By theorem 8, E (and therefore its quadratic twist) must be ordinary. The algorithm is given below:

```
Input: $p$, a prime, and $N$ a positive integer
Output: An elliptic curve $E(\mathbb{F}_p)$ where $\#E(\mathbb{F}_p) = N$
$t := p + 1 - N$;
$D$ = square free part of $t^2 - 4p$;
$H_D(x)$ = 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
```

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 $1, \zeta, \zeta^2, \ldots, \zeta^5$, for ζ, 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 $1, \zeta, \ldots \zeta^3$, for ζ, 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 $\left(\frac{D}{r}\right) = 1$. 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. $p + 1 - t \equiv 0 \mod r$. This means that $r \Big| \#E(\mathbb{F}_p) \implies$ there is a subgroup of size r by the characterization of finitely generated abelian groups
3. p is a primitive kth 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.

If we satisfy the above 3 conditions for p, t, we can apply the CM method to construct the desired curve E. First, we choose g, a primitive kth root of unity mod r. We know that $t - 1 \equiv p \equiv g \mod r$. Using (1), we see that $\frac{(t^2 - f^2 D)}{4} = p$. We can set $a = 2^{-1}(g+1) \mod r$ (as integers). Then, $2a \equiv g+1 \equiv t \mod r \implies a^2 \equiv \frac{t^2}{4} \mod r$. We can also set $f_0 = \frac{2(a-1)}{\sqrt{D}} \mod r$. Suppose $p = \frac{(t^2 - f_0^2 D)}{4}$ is prime, and $t = 2a$. Then $p + 1 - t \equiv a^2 - (a-1)^2 + 1 - t \equiv 2a - 1 + 1 - t \equiv 0 \mod r$, 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 $\left(\frac{D}{r}\right) = 1$
Output: $p$, prime, $t$, trace of Frobenius
$g :=$ primitive $k$th root of unity mod $r$
$a := 2^{-1}(g+1) \mod r$ (as integers)
$f = \frac{2(a-1)}{d}$ (as integers where $d \equiv \sqrt{D} \mod r$)
$t := 2a$
$p = \frac{(t^2 - f^2 D)}{4}$
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 $t \not\equiv 0 \mod p$. The last equation is satisfied since $t > 0$ and $p > t$. Therefore, E exists.

3.3 Dupont-Enge-Morain Method

As is the case in the Cocks-Pinch method, we still need to find parameters k, r, D, p, t satisfying the three conditions. The main idea behind the Dupont-Enge-Morain (DEM) Method is to fix an embedding degree k and simultaneously compute the prime r and D using resultants. We define the resultant of two polynomials $f(x), g(x) \in \mathbb{F}[x]$ as

$$\mathrm{Res}(f, g) = \prod (r_f - r_g)$$

where r_f and r_g are the roots of $f(x)$ and $g(x)$ in $\overline{\mathbb{F}}$. From the definition, it is clear that $\mathrm{Res}(f, g) = 0 \iff f$ and g have a common root in $\overline{\mathbb{F}}$. We can replace condition (3) of the Cocks-Pinch method with $r\Big|\Phi_k(q) \iff r\Big|\Phi_k(t-1)$ (if condition 2 also holds), where $\Phi_k(x)$ is the kth cyclotomic polynomial. Suppose that $-f^2D + (t-2)^2 \equiv 0 \mod r$. Then $0 \equiv -f^2D + t^2 - 4t + 4 \equiv 4p - 4t + 4 \equiv 4(p+1-t) \mod r \implies p+1-t \equiv 0 \mod r$ since $\gcd(4, r) = 1$, and we can assume that $r \neq 2$. If we can find $a \in \mathbb{Z}$ such that $r = \mathrm{Res}(\Phi_k(x-1), a + (x-2)^2)$ is a prime, then $\mathrm{Res}(\Phi_k(x-1), a + (x-2)^2) \equiv 0 \mod r \implies \Phi_k(x-1)$ and $a + (x-2)^2$ have a common root in $\overline{\mathbb{F}_r}$ so that $g(x) = \gcd(\Phi_k(x-1), a + (x-2)^2) \in \mathbb{F}_r[x]$ has a root in $\overline{\mathbb{F}_r}$. As it turns out, $g(x)$ will have a root in $\mathbb{F}_r$. [TAX10] If we let t be this root, then we see that $\Phi_k(t-1) \equiv 0 \mod r$ and that $a + (t-2)^2 \equiv 0 \mod r$. If $\exists i \in \mathbb{Z}^+$ such that $p = \frac{(t+ir)^2+a}{4}$ is a prime, then $p \equiv \frac{t^2+a}{4} \mod r$ so that $p + 1 - t \equiv 0 \mod r$ by an earlier argument. Letting $-f^2D = a$, we see that the three conditions are satisfied, and therefore we can use the CM method to construct the desired elliptic curve E. By the same argument used in the Cocks-Pinch method, we see that $|t| \leq 2\sqrt{p}$. The algorithm is given below in pseudocode:

```
Input: $k$, embedding degree
Output: $r$, subgroup size,$D$, CM discriminant, $p$, prime, $t$, trace of Frobenius
$a$ :=random integer with small squarefree part
while $r$ is not prime do
    $r = \mathrm{Res}(\Phi_k(x-1), a + (x-2)^2$
end
$D$ := squarefree part of $a$
$g(x) = \gcd(\Phi_k(x-1), a + (x-2)^2)$
$t$ :=any root of $g(x) \in \mathbb{F}_r$. while $p$ is not prime do
    $p = \frac{(t+ir)^2+a}{4}$ for some $i \in \mathbb{Z}^+$
end
return $r, D, p, t$
```

The Cocks-Pinch method and DEM method are both very similar. The Cocks-Pinch method is preferable primarily because it allows the user to specify the subgroup size (which determines the security level of the curve), whereas the DEM method does not have this flexibility.

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 ρ 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 $k \mod q_i^{e_i}$ 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.

5 Conclusion

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.