Elliptic Curve Cryptography – Survey

This survey requires from the reader knowledge in field theory, group theory and number theory.

Definitions
An elliptic curve over a field $\mathbb{F}$ is the set of pairs, or points, $(x, y)$, $x \in \mathbb{F}, y \in \mathbb{F}$, that satisfy the equation:
$$E: y^2 + ay = x^3 + bx^2 + cxy + dx + e,$$ where $a, b, c, d, e \in \mathbb{F}$. $E(\mathbb{F})$ denotes all those points, with the infinity point $\infty$.

When the characteristic of $\mathbb{F} \neq 2,3$ then we can write $E: y^2 = x^3 + ax + b$ where $a, b \in \mathbb{F}$.
$$\Delta = -16(4a^3 + 27b^2)$$ is called the discriminant of $E(\mathbb{F})$. When $\Delta \neq 0$ a curve is called nonsingular.

Normally it is drawn over the field $\mathbb{R}$. The following, for example, is the elliptic curve $y^2 = x^3 + 3x + 5$ over $\mathbb{R}$:

![Elliptic Curve](image)

The group over an elliptic curve $E$ over a field $\mathbb{F}$ has the elements $E(\mathbb{F})$.

- It’s identity is $\infty$, i.e. for each point $P \in E(\mathbb{F})$: $P + \infty = \infty + P$.
- The negation of a point $P$, denoted $-P$, is the one symmetrical to it in respect to the x-axis (in finite fields, the inverse of $(x, y)$ is $(x, -y)$, where the negation of $y$ is taken in the respective field).
  - $\infty = -\infty$
- The addition of 2 points $P, Q$ is performed by drawing the line connecting $P$ with $Q$, finding it’s 3rd intersection with $E$ - call it $R$, and then: $P + Q = -R$ (Notice that this can be done over a finite field $\mathbb{F}$ too. The line through $P = (r, s), Q = (u, v)$ can be written as $y - s = \frac{v-s}{u-r}(x - r)$ - we can divide in any field – and the 3rd intersection is found by solving the system of equations: $y - s = \frac{v-s}{u-r}(x - r)$ and $E$).
  - If a 3rd intersection doesn’t exist, we choose $R = \infty$.
  - In order to add $P$ with itself, we will draw the tangent to $E$ through $P$, and continue in the same way. The condition $\Delta \neq 0$ is required so that $P$ won’t have 2 tangent lines.

In this survey we are only considering elliptic curves $E$ over finite fields $\mathbb{F}_p$, where $p > 2$ is a prime.
Cryptography

Now, having defined a group, we can use it for cryptographic protocols. A common example for this is the ElGamal encryption and decryption scheme, which can use any cyclic group. Another example is the Diffie-Hellman key exchange – which also uses any cyclic group. We can choose one point $P$ in $E(\mathbb{F}_p)$, and the subgroup of the curve that is generated by this point can be used for those protocols.

Elliptic curve cryptography (ECC) is considered to be somewhat better than the more commonly used RSA. It is better in the sense that in order to achieve the same level of security, ECC requires a key of much smaller size than RSA. Here is a small comparison table:

<table>
<thead>
<tr>
<th>RSA</th>
<th>ECC</th>
</tr>
</thead>
<tbody>
<tr>
<td>428</td>
<td>110</td>
</tr>
<tr>
<td>521</td>
<td>119</td>
</tr>
<tr>
<td>768</td>
<td>144</td>
</tr>
<tr>
<td>1024</td>
<td>163</td>
</tr>
<tr>
<td>2048</td>
<td>222</td>
</tr>
</tbody>
</table>

Both of the cryptographic schemes mentioned earlier are based on the assumption of hardness of solving the discrete logarithm problem: given $g^x = h$ for 2 elements $g, h$ in a cyclic group $G = \langle g \rangle$, find $x$.

Those schemes are stronger with ECC since (unlike for number theory based groups) there is no known sub-exponential algorithm for solving the discrete logarithm problem for the group of an elliptic curve.

Good and Bad Curves for Cryptography

Sadly, even though no sub-exponential algorithm for solving the discrete logarithm for $E(\mathbb{F}_p)$ is known, not any curve $E(\mathbb{F}_p)$ will provide us with good enough security. There are several attacks to consider:

Brute Force

The simplest attack to find the logarithm of a point $Q$ in the group $\langle P \rangle$ (generated by $P$) is to try all possible values for $x$, one by one. In order for the attacker to fail, we want to have $ord(P)$ large enough so that it will be impossible.

Pohlig – Hellman

Suppose $ord(P) = n = \prod_{j=1}^{k} p_j^{a_j}$, where $p_j$ are primes. This attack reduces computing the discrete log of $Q$ in $\langle P \rangle$ to computing discrete logarithms of $a_j$ points in groups with orders $p_j$, for each $1 \leq j \leq k$. This gives a total of $O(\log n)$ discrete logarithms in smaller groups. In order to increase resistance to this attack, $ord(P)$ not only needs to be large, but also be divisible by a large enough prime.

Weil and Tate pairing

Suppose $gcd(ord(P), p) = 1$, and let $k$ be the smallest natural number for which: $p^k \equiv 1 (mod \ ord(P))$. The 2 attacks form isomorphisms from $\langle P \rangle$ to some subgroup of the multiplicative group of $\mathbb{F}_{p^k}^\times$. In this group we could use some sub-exponential algorithm to compute the discrete log, since this group is much simpler for small $k$. In order to increase resistance to this attack, $ord(P)$ shouldn’t divide $p^k - 1$ for relatively small $k$, or $p$ should be increased even further.
Point Counting – Schoof’s Algorithm

Those attacks and others show that before settling on what curve we will use, we should first carefully study the order of the group we chose. In order to do that we need, at least, to be able to count how many points are on a nonsingular $E(F_q)$. The following algorithm does just that.

But first we require some theorems and definitions:

**Definitions:** Let $\overline{F_q}$ denote the algebraic closure of $F_q$.

A point $P$ is named an $m$-torsion point if $mP = \infty$ (where $mP$ denotes the addition of $P$ $m$ times). The set of $m$-torsion points in a curve $E$ is denoted $E[m]$. This is a subgroup of $E(\overline{F_q})$.

The set of endomorphisms of a curve $E$, denoted by $\text{End}(E)$ is the set of homomorphisms from the group of $E$ to itself that are given by rational functions. This set forms a ring, where addition of $\phi, \sigma \in \text{End}(E)$ is: $(\phi + \sigma)(P) = \phi(P) + \sigma(P)$, and multiplication is done by composition.

**Hasse’s Theorem:** Let $E(\overline{F_q})$ be an elliptic curve, $N = |E(\overline{F_q})|$. Then $|N - q - 1| \leq 2\sqrt{q}$.

**The Frobenius Map:** Let’s consider the following function $\pi: (x, y) \rightarrow (x^q, y^q)$ where $x, y \in \overline{F_q}$. We can see that $\pi$ is an endomorphism of $E(\overline{F_q})$ and in fact an identity on $E(\overline{F_q})$. The characteristic equation for the Frobenius map is: $\pi^2 - t\pi + q = 0$, where $t = |N - q - 1|$.

**Division Polynomials:**

We define the following polynomials in $\mathbb{Z}[a, b][x, y]$:

\[
\begin{align*}
\psi_0 &= 0, \quad \psi_1 = 1, \quad \psi_2 = 2y, \quad \psi_3 = 3x^4 + 6ax^2 + 12bx - a^2 \\
\psi_4 &= 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3) \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \quad m \geq 2 \\
\psi_{2m} &= (\psi_{m+2}\psi_{m-2}\psi_{m+1}^2)\psi_m/2y, \quad m \geq 3
\end{align*}
\]

The polynomial $\psi_m$ is called the $m$-th division polynomial. When calculating these polynomials we can keep $\text{deg}(y) \leq 1$, because we can use the relation $y^2 = x^3 + ax + b$, and $\text{deg}(x) = (m^2 - 1)/2$.

The division polynomials have the property that for every point $P \neq \infty$, $\psi_m(P) = 0 \iff P$ is an $m$-torsion point. Also it is easy to write $rP$ as a pair of rational functions in $x$ and $y$, using division polynomials. (The exact definitions can be found in [3].) This essentially means that the map $P \rightarrow rP$ is in $\text{End}(E)$.

**Schoof’s idea**

Assume our elliptic curve is $E(\overline{F_q})$. Let: $t = |N - q - 1|$. By Hasse’s theorem, it is sufficient to calculate $t$ (mod $M$), where $M \geq 4\sqrt{q}$. Now if we find $t$ (mod $l_i$), where $\prod l_i \geq 4\sqrt{q}$ and $l_i$ are pair-wise coprime, we can utilize the Chinese Remainder Theorem to easily find $t$ (mod $\prod l_i$), and therefore find $t$. From $t$ we then can calculate $N$.

For the rest of this section let $l$ be a small prime such that $l \neq \text{char}(F_q)$, $2$.

Recall that our goal is to find some $\bar{t}$ such that: $\bar{t} \equiv t$ (mod $l$). Define $\bar{q}$ to be the unique integer such that $\bar{q} \equiv q$ (mod $l$) and $|\bar{q}| \leq \frac{l}{2}$. If $P = (x, y) \in E(\overline{F_q})$ is an $l$-torsion point, then $qP = \bar{q}P$. Also note that $P$ and $\pi(P)$ have the same order. Using the characteristic equation of the Frobenius map, we know that for every $l$-torsion point $P$: $(x^{\bar{q}2}, y^{\bar{q}2}) + \bar{q}(x, y) \equiv \bar{t}(x^{\bar{q}}, y^{\bar{q}})$ (mod $l$). The idea is to find a solution for this equation.
Main Algorithm

We will consider 3 different cases: \((x^q^2, y^q^2) \neq \pm \bar{q}(x, y)\); \((x^q^2, y^q^2) = \bar{q}(x, y)\); \((x^q^2, y^q^2) = -\bar{q}(x, y)\).

Because the first case is the most common one, we start with it.

1. Find a point \(P\) such that \(\psi_1(P) = 0\). Recall that this implies \(P\) is of order \(l\). We then consider \((x^q^2, y^q^2) \neq \pm \bar{q}(x, y)\). If we are incorrect, then we will not be able to find an appropriate \(\bar{t}\) and we will know that we are in the second case.

2. For every \(\bar{t} = \frac{1}{2} \,(1 - t)\) we check whether the 2 coordinates of \((x^q^2, y^q^2) + \bar{q}(x, y)\) and \(\bar{t}(x, y)\) are equal. If they are also equal then we have found \(\bar{t}\), and end the loop. Otherwise we continue. If we have exhausted all the choices for \(\bar{t}\) then we know we are in the second case.

3. Assume that \((x^q^2, y^q^2) = \bar{q}(x, y)\). Using the Frobenius map we obtain the following two congruencies:

\[
2\bar{q}(x, y) \equiv \bar{t}\bar{t} (x, y) \pmod{2l} \quad \text{and} \quad 2\bar{q}(x, y) \equiv \bar{t}(x, y) \pmod{2l}
\]

We then conclude that \(\bar{q}\) is a square modulo \(l\). Let \(\bar{q} \equiv w^2 \pmod{l}\). Now we can rewrite and get:

\[
\pi^2(x, y) - \bar{q}(x, y) \equiv (\pi - w)(\pi + w)(x, y) \equiv \infty \pmod{l}
\]

If \((\pi - w)(x, y) \equiv \infty\) then \(\pi^2(x, y) \equiv \pi + w \equiv (q - \bar{t}w + q)(x, y)\) and we get \(\bar{t} \equiv 2w \pmod{l}\). Similarly if \((\pi + w)(x, y) \equiv \infty\) then \(\bar{t} \equiv -2w \pmod{l}\).

4. If we failed during the 4th step, especially if we couldn’t find \(\bar{q} \equiv w^2 \pmod{l}\), then \((x^q^2, y^q^2) = -\bar{q}(x, y)\).

In this case \((x^q^2, y^q^2) + \bar{q}(x, y) \equiv \infty \pmod{l}\) and \(\bar{t} \equiv 0 \pmod{l}\).

The case: \(l = 2\)

Since \(q\) is odd, \(q + 1 - t \equiv t \pmod{2}\) and therefore \(t \equiv 0 \pmod{2}\) iff \(E(F_q)\) has a 2-torsion point. This is true if and only if \(y^2 = x^3 + ax + b\) has a root in \(F_q\).

All these calculations are done using representations of points as rational functions in \(x\) and \(y\) (which is possible, due to the fact that the maps \(P \rightarrow \tau P\) and \(\pi\) are in \(End(E)\)). Also, because we are only interested in the case for every \(l\)-torsion point, we can do all the calculations modulo \(\psi_1\) and thus the degrees of all the polynomials involved are bounded.

Creating Curves – Complex Multiplication Algorithm

Recall that our main objective is to find a cryptographically strong elliptic curve. If we only use Schoof’s algorithm, we will end up generating many curves and testing their cardinalities, until we find one that satisfies us. However, since Schoof’s Algorithm isn’t fast enough to run it many times, we need an algorithm which will generate curves in some manner that would help us find a good curve faster (not just generate random curves until we are lucky). This algorithm tries to do just that.

Once more, we will require some additional theory.

**Definitions:**

The function \(j(E) = -1728(4a^3)/\Delta\) is called the \(j\)-invariant of the curve \(E\): \(y^2 = x^3 + ax + b\). Notice that \(j(E)\) of a curve \(E(K)\) is in the field \(K\).

A **number field** is a finite extension of \(\mathbb{Q}\). A number \(x\) from a number field is called an **algebraic integer**, if there is a monic polynomial \(f \subseteq \mathbb{Z}[x]\) such that \(f(x) = 0\).

An **order** is a sub-ring of finite index of the ring of algebraic integers in some field. Consider an elliptic curve \(E\) over the field \(\mathbb{C}\). Recall that \(End(E)\) contains all maps \(P \rightarrow \tau P\). Hence \(End(E)\) contains (as a sub-ring) an isomorphic copy of \(\mathbb{Z}\). It is known that if \(End(E)\) is not itself isomorphic to \(\mathbb{Z}\), then it is isomorphic to an order in an imaginary quadratic number field. In this case \(E\) is said to have complex
multiplication, or is a CM curve. In this case, in fact, we can write (Deuring's Theorem): $\text{End}(E) \cong \mathbb{Z} + \tau \mathbb{Z}$, where $\tau$ is a complex algebraic number of degree 2, where $\text{Im}(\tau) > 0$.

A negative integer $D$ such that it’s odd part is square-free, and $D \equiv 3, 4, 7, 8, 11, 15 \pmod{16}$ is called a fundamental discriminant.

Throughout this part $D$ always denotes a fundamental discriminant.

**Quadratic forms:** A quadratic form is a triplet $(a, b, c)$ of integers. The triplet represents an integer $n$ if we can find integers $x, y$ such that $ax^2 + bxy + cy^2 = n$.

Two quadratic forms $(a', b', c')$, $(a, b, c)$ are called equivalent if we can find integers $\alpha, \beta, \gamma, \delta$ such that: $\alpha \delta - \beta \gamma = 1$, $a' = a\alpha^2 + b\alpha \gamma + c\gamma^2$, $c' = a\beta^2 + b\beta \delta + c\delta^2$ and $b' = 2\alpha \beta + b(\alpha \delta + b\gamma + 2c\delta)$. The discriminant of a quadratic form $(a, b, c)$ is $b^2 - 4ac$. Equivalent quadratic forms have the same discriminant (however the converse is not correct).

A binary quadratic form $(a, b, c)$ is called primitive, if $\gcd(a, b, c) = 1$.

A binary quadratic form $(a, b, c)$ is called reduced, if $-a < b \leq a < c$ or $0 \leq b \leq a = c$.

A theorem by Gauss states that reduced forms are representatives of equivalency classes (no 2 reduced forms are equivalent, each quadratic form is equivalent to some reduced form).

The amount of reduced binary quadratic forms of discriminant $D$ is denoted $h(D)$.

**Hilbert class polynomials:** The Hilbert class polynomial of a fundamental discriminant $D$ has degree $h(D)$ and coefficients in $\mathbb{Z}$. It is given by: $H_D(x) = \prod (x - j(\alpha))$, where we iterate over all different roots with $\text{Im}(\alpha) > 0$ of polynomials $ax^2 + bx + c$, where $(a, b, c)$ is a reduced quadratic form of discriminant $D$. Also, $j(\alpha) = \frac{(256h(\alpha)+1)^3}{h(\alpha)}$, $h(\alpha) = \frac{\Delta(2\alpha)}{\Delta(\alpha)}$, $\Delta(\alpha) = q \left(1 + \sum_{n \geq 1} (-1)^n \left( q^{n(3n-1)/2} + q^{n(3n+1)/2} \right) \right)^{24}$ and $q = e^{2\pi i \alpha}$.

$H_D(x)$ is the minimal polynomial of $j(\alpha)$.

**Main Theorems**

1. If an elliptic curve $E$, when considered over $\mathbb{C}$, has complex multiplication, and $\text{End}(E) \cong \mathbb{Z} + \tau \mathbb{Z}$, such that $\tau$ is a root of some polynomials $ax^2 + bx + c$, where $(a, b, c)$ is a reduced quadratic form of discriminant $D$, then $j(E) = j(\tau)$. That means that $j(E)$ is a root of $H_D(x)$.

Recall that when we consider the curve over a field $\mathbb{K}$, the $j$-invariant is in $\mathbb{K}$. So if we consider $E$ over $\mathbb{F}_p$, then it’s $j$-invariant is a root in $\mathbb{F}_p$ of $H_D(x)$. Therefore we can compute it without knowing the coefficients of the curve.

2. The order of a curve over $\mathbb{F}_p$, that has complex multiplication with discriminant $D$, is $p + 1 \pm t$, where $t$ is a solution to $4p = t^2 - D$ $y^2$. That Diophantine equation is quickly solved with Cornacchia’s algorithm.

3. Knowing the $j$-invariant of a curve $E$ over $\mathbb{F}_p$, that has complex multiplication with discriminant $D$, it is easy to construct a curve with order $p + 1 + t$, $t$ from theorem 2.

Simply choose the curve: $y^2 = x^3 + 3kc^2x + 2kc^3$ where $c$ is some element in $\mathbb{F}_p$ and $k = \frac{-1}{1728 - j}$. (We obviously can’t have $j = 0, 1728$ here, but we ignore those cases because they might be cryptographically weaker). Also, given a curve $y^2 = x^3 + ax + b$, it’s twist is a curve $y^2 = x^3 + ac^2x + bc^3$, where $c$ is some quadratic non-residue in $\mathbb{F}_p$. That means that if the order of the first curve is $p + 1 + t$, then the order of the second curve is $p + 1 - t$, and vice-versa.
Generating a Cryptographically Strong Curve

1. Choose a random prime \( p \), which will be our field \( \mathbb{F}_p \) (This is done easily by choosing a random number with the wanted amount of bits, and incrementing it until it's a prime. Primality checking schemes are well-known. The process will quickly stop with high probability due to PNT).

2. Repeat the following for fundamental discriminants \( D \):

3. Find solutions to \( 4p = x^2 - Dy^2 \) (using Cornacchia's algorithm), and compute \( p + 1 \pm x \). Those are the possible orders of our curve. Continue when we find an order \( p + 1 \pm x \) that passes our criteria for cryptographic strength.

4. Find a root \( j \) over \( \mathbb{F}_p \) of the polynomial \( H_D(x) \). If no such root exists, return to 3.

5. Compute a CM curve \( E \) with \( j \)-invariant \( j \). We know that its' order is \( p + 1 \pm x \).

6. To test which is it, take a random point in \( E \), and multiply it by \( p + 1 + x \). If we didn't get \( \infty \), the order is \( p + 1 - x \). If we did, the order is probably \( p + 1 + x \). Repeat several times to make sure.

7. If we want the second order (not the one \( E \) has), we compute the twist of \( E \) using the formula.

Remarks

- The above scheme for finding a cryptographically strong elliptic curve can be altered to choosing \( D \) first and then taking random primes until the algorithm ends. It is unclear which gives better curves.
- It is common belief that fundamental discriminants \( D \) with relatively small \( h(D) \) are cryptographically weak and should therefore be avoided, however there is no attack that supports this belief.
- The computation of \( j(\alpha) \) in Hilbert's polynomials obviously can't be done accurately, since it's an infinite series. Each \( j(\alpha) \) should be computed with high enough precision, which seems unachievable. We instead compute Weber's polynomial. This is a minimal polynomial of some other value which is closely related to \( j(\alpha) \). The roots of Hilbert's polynomial can be computed from the roots of Weber's polynomial. However, Weber's polynomial has proved to require far less precision, and it's coefficients are normally much smaller. The formulas for computing Weber's polynomials are slightly more complicated and can be found in [4].

Bibliography

2. "Prime Numbers – A computational Perspective" – R.Crandall, C.Pomerance
3. "Schoof’s Algorithm for Counting Points on \( E(F_q) \) " – G. Musiker
4. "Elliptic Curves in Cryptography" – I.Blake, G.Seroussi, N.Smart