Elliptic Curve Cryptography

Elliptic Curves

An elliptic curve is a cubic equation of the form:

\[ y^2 + axy + by = x^3 + cx^2 + dx + e \]

where \( a, b, c, d \) and \( e \) are real numbers.

A special addition operation is defined over elliptic curves, and this with the inclusion of a point \( O \), called point at infinity. If three points are on a line intersect an elliptic curve, their sum is equal to this point at infinity \( O \) (which acts as the identity element for this addition operation).

Figure 1 shows the elliptic curves \( y^2 = x^3 + 2x + 5 \) and \( y^2 = x^3 - 2x + 1 \).

Elliptic Curves over Galois Fields

An elliptic group over the Galois Field \( E_p(a, b) \) is obtained by computing \( x^3 + ax + b \mod p \) for \( 0 \leq x < p \). The constants \( a \) and \( b \) are non-negative integers smaller than the prime number \( p \) and must satisfy the condition:

\[ 4a^3 + 27b^2 \mod p \neq 0 \]

For each value of \( x \), one needs to determine whether or not it is a quadratic residue. If it is the case, then there are two values in the elliptic group. If not, then the point is not in the elliptic group \( E_p(a, b) \).
Example (construction of an elliptic group):

Let the prime number $p = 23$ and let the constants $a = 1$ and $b = 1$ as well. We first verify that:

$$4a^3 + 27b^2 \mod p = 4 \times 1^3 + 27 \times 1^2 \mod 23$$
$$4a^3 + 27b^2 \mod p = 4 + 27 \mod 23 = 31 \mod 23$$
$$4a^3 + 27b^2 \mod p = 8 \neq 0$$

We then determine the quadratic residues $Q_{23}$ from the reduced set of residues $Z_{23} = \{1, 2, 3, \ldots, 21, 22\}$:

<table>
<thead>
<tr>
<th>$x^2 \mod p$</th>
<th>$(p-x)^2 \mod p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1^2 \mod 23$</td>
<td>$22^2 \mod 23$</td>
</tr>
<tr>
<td>$2^2 \mod 23$</td>
<td>$21^2 \mod 23$</td>
</tr>
<tr>
<td>$3^2 \mod 23$</td>
<td>$20^2 \mod 23$</td>
</tr>
<tr>
<td>$4^2 \mod 23$</td>
<td>$19^2 \mod 23$</td>
</tr>
<tr>
<td>$5^2 \mod 23$</td>
<td>$18^2 \mod 23$</td>
</tr>
<tr>
<td>$6^2 \mod 23$</td>
<td>$17^2 \mod 23$</td>
</tr>
<tr>
<td>$7^2 \mod 23$</td>
<td>$16^2 \mod 23$</td>
</tr>
<tr>
<td>$8^2 \mod 23$</td>
<td>$15^2 \mod 23$</td>
</tr>
<tr>
<td>$9^2 \mod 23$</td>
<td>$14^2 \mod 23$</td>
</tr>
<tr>
<td>$10^2 \mod 23$</td>
<td>$13^2 \mod 23$</td>
</tr>
<tr>
<td>$11^2 \mod 23$</td>
<td>$12^2 \mod 23$</td>
</tr>
</tbody>
</table>

Therefore set of $\frac{p-1}{2} = 11$ quadratic residues $Q_{23} = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$.

Now, for $0 \leq x < p$, compute $y^2 = x^3 + x + 1 \mod 23$ and determine if $y^2$ is in the set of quadratic residues $Q_{23}$:

<table>
<thead>
<tr>
<th>$x$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>$y^2$</td>
<td>1</td>
<td>3</td>
<td>11</td>
<td>8</td>
<td>0</td>
<td>16</td>
<td>16</td>
<td>6</td>
<td>15</td>
<td>3</td>
<td>22</td>
<td>9</td>
</tr>
<tr>
<td>$y^2 \in Q_{23}$?</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>$y_1$</td>
<td>1</td>
<td>7</td>
<td>10</td>
<td>0</td>
<td>4</td>
<td>4</td>
<td>11</td>
<td>7</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$y_2$</td>
<td>22</td>
<td>16</td>
<td>13</td>
<td>0</td>
<td>19</td>
<td>19</td>
<td>12</td>
<td>16</td>
<td>20</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The elliptic group $E_p(a, b) = E_{23}(1, 1)$ thus include the points (including also the additional single point $(4, 0)$):

$$
E_{23}(1, 1) = \left\{ \begin{array}{c}
(0, 1) & (0, 22) & (1, 7) & (1, 16) & (3, 10) & (3, 13) & (4, 0) \\
(5, 4) & (5, 19) & (6, 4) & (6, 19) & (7, 11) & (7, 12) & (9, 7) \\
(9, 16) & (11, 3) & (11, 20) & (12, 4) & (12, 19) & (13, 7) & (13, 16) \\
(17, 3) & (17, 20) & (18, 3) & (18, 20) & (19, 5) & (19, 18)
\end{array} \right\}
$$

Figure 2 shows a scatterplot of elliptic group $E_p(a, b) = E_{23}(1, 1)$.
Addition and multiplication operations over elliptic groups

Let the points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be in the elliptic group $E_p(a, b)$, and $O$ is the point at infinity. The rules for addition over the elliptic group $E_p(a, b)$ are:

1. $P + O = O + P = P$

2. If $x_2 = x_1$ and $y_2 = -y_1$, that is $P = (x_1, y_1)$ and $Q = (x_2, y_2) = (x_1, -y_1) = -P$, then $P + Q = O$.

3. If $Q \neq -P$, then the sum $P + Q = (x_3, y_3)$ is given by:

$$
\begin{align*}
x_3 &= \lambda^2 - x_1 - x_2 \mod p \\
y_3 &= \lambda(x_1 - x_3) - y_1 \mod p
\end{align*}
$$

where

$$
\lambda \triangleq \begin{cases} 
\frac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q \\
\frac{3x_1^2 + a}{2y_1} & \text{if } P = Q
\end{cases}
$$

Example (Multiplication over an elliptic curve group):

The multiplication over an elliptic curve group $E_p(a, b)$ is the equivalent of the modular exponentiation in RSA.

Let $P = (3, 10) \in E_{23}(1, 1)$. Then $2P = (x_3, y_3)$ is equal to:

$$
2P = P + P = (x_1, y_1) + (x_1, y_1)
$$

Since $P = Q$ and $x_2 = x_1$, the values of $\lambda$, $x_3$ and $y_3$ are given by:

$$
\begin{align*}
\lambda &= \frac{3x_1^2 + a}{2y_1} \mod p = \frac{3 \times (3^2) + 1}{2 \times 10} \mod 23 = 5 \mod 23 = 6 \\
x_3 &= \lambda^2 - x_1 - x_2 \mod p = 6^2 - 3 - 3 \mod 23 = 30 \mod 23 = 7 \\
y_3 &= \lambda(x_1 - x_3) - y_1 \mod p = 6 \times (3 - 7) - 10 \mod 23 = -34 \mod 23 = 12
\end{align*}
$$

Therefore $2P = (x_3, y_3) = (7, 12)$.

The multiplication $kP$ is obtained by doing the elliptic curve addition operation $k$ times by following the same additive rules.
<table>
<thead>
<tr>
<th>$k$</th>
<th>$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ (if $P \neq Q$) or $\lambda = \frac{3x_1^2 + a}{2y_1}$ if $P = Q$</th>
<th>$x_3$</th>
<th>$y_3$</th>
<th>$kP$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ (if $P \neq Q$) or $\lambda = \frac{3x_1^2 + a}{2y_1}$ if $P = Q$</td>
<td>$\lambda^2 - x_1 - x_2$ mod 23</td>
<td>$\lambda(x_1 - x_3) - y_1$ mod 23</td>
<td>$(x_3, y_3)$</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>7</td>
<td>12</td>
<td>(3, 10)</td>
</tr>
<tr>
<td>3</td>
<td>12</td>
<td>19</td>
<td>5</td>
<td>(19, 5)</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>17</td>
<td>3</td>
<td>(17, 3)</td>
</tr>
<tr>
<td>5</td>
<td>11</td>
<td>9</td>
<td>19</td>
<td>(9, 16)</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>12</td>
<td>4</td>
<td>(12, 4)</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>11</td>
<td>3</td>
<td>(11, 3)</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>13</td>
<td>16</td>
<td>(13, 16)</td>
</tr>
<tr>
<td>9</td>
<td>19</td>
<td>0</td>
<td>1</td>
<td>(0, 1)</td>
</tr>
<tr>
<td>10</td>
<td>3</td>
<td>6</td>
<td>4</td>
<td>(6, 4)</td>
</tr>
<tr>
<td>11</td>
<td>21</td>
<td>18</td>
<td>20</td>
<td>(18, 20)</td>
</tr>
<tr>
<td>12</td>
<td>16</td>
<td>5</td>
<td>4</td>
<td>(5, 4)</td>
</tr>
<tr>
<td>13</td>
<td>20</td>
<td>1</td>
<td>7</td>
<td>(1, 7)</td>
</tr>
<tr>
<td>14</td>
<td>13</td>
<td>4</td>
<td>0</td>
<td>(0, 0)</td>
</tr>
<tr>
<td>15</td>
<td>13</td>
<td>1</td>
<td>16</td>
<td>(1, 16)</td>
</tr>
<tr>
<td>16</td>
<td>20</td>
<td>5</td>
<td>19</td>
<td>(5, 19)</td>
</tr>
<tr>
<td>17</td>
<td>16</td>
<td>18</td>
<td>3</td>
<td>(18, 3)</td>
</tr>
<tr>
<td>18</td>
<td>21</td>
<td>6</td>
<td>19</td>
<td>(6, 19)</td>
</tr>
<tr>
<td>19</td>
<td>3</td>
<td>0</td>
<td>22</td>
<td>(0, 22)</td>
</tr>
<tr>
<td>20</td>
<td>19</td>
<td>13</td>
<td>7</td>
<td>(13, 7)</td>
</tr>
<tr>
<td>21</td>
<td>2</td>
<td>11</td>
<td>20</td>
<td>(11, 20)</td>
</tr>
<tr>
<td>22</td>
<td>7</td>
<td>12</td>
<td>19</td>
<td>(12, 19)</td>
</tr>
<tr>
<td>23</td>
<td>1</td>
<td>9</td>
<td>7</td>
<td>(9, 7)</td>
</tr>
<tr>
<td>24</td>
<td>11</td>
<td>17</td>
<td>20</td>
<td>(17, 20)</td>
</tr>
<tr>
<td>25</td>
<td>4</td>
<td>19</td>
<td>18</td>
<td>(19, 18)</td>
</tr>
<tr>
<td>26</td>
<td>12</td>
<td>7</td>
<td>11</td>
<td>(7, 11)</td>
</tr>
<tr>
<td>27</td>
<td>6</td>
<td>3</td>
<td>13</td>
<td>(3, 13)</td>
</tr>
</tbody>
</table>
Elliptic Curve Encryption

Elliptic curve cryptography can be used to encrypt plaintext messages, $M$, into ciphertexts. The plaintext message $M$ is encoded into a point $P_M$ from the finite set of points in the elliptic group, $E_p(a, b)$. The first step consists in choosing a generator point, $G \in E_p(a, b)$, such that the smallest value of $n$ such that $nG = O$ is a very large prime number. The elliptic group $E_p(a, b)$ and the generator point $G$ are made public.

Each user selects a private key, $n_A < n$ and computes the public key $P_A$ as: $P_A = n_A G$. To encrypt the message point $P_M$ for Bob ($B$), Alice ($A$) chooses a random integer $k$ and computes the ciphertext pair of points $P_C$ using Bob’s public key $P_B$:

$$P_C = [(kG), (P_M + kP_B)]$$

After receiving the ciphertext pair of points, $P_C$, Bob multiplies the first point, $(kG)$ with his private key, $n_B$, and then adds the result to the second point in the ciphertext pair of points, $(P_M + kP_B)$:

$$(P_M + kP_B) - [n_B(kG)] = (P_M + kn_BG) - [n_B(kG)] = P_M$$

which is the plaintext point, corresponding to the plaintext message $M$. Only Bob, knowing the private key $n_B$, can remove $n_B(kG)$ from the second point of the ciphertext pair of points, i.e. $(P_M + kP_B)$, and hence retrieve the plaintext information $P_M$.

Example (Elliptic curve encryption):

Consider the following elliptic curve:

$$y^2 = x^3 + ax + b \mod p$$

that is: $a = -1$, $b = 188$, and $p = 751$. The elliptic curve group generated by the above elliptic curve is then $E_p(a, b) = E_{751}(-1, 188)$.

Let the generator point $G = (0, 376)$. Then the multiples $kG$ of the generator point $G$ are (for $1 \leq k \leq 751$):

- $G = (0, 376)$
- $2G = (1, 376)$
- $3G = (375, 375)$
- $4G = (2, 373)$
- $5G = (188, 657)$
- $6G = (6, 390)$
- $7G = (667, 571)$
- $8G = (121, 39)$
- $9G = (582, 736)$
- $10G = (57, 332)$
- $762G = (328, 569)$
- $763G = (677, 185)$
- $764G = (196, 681)$
- $765G = (417, 320)$
- $766G = (3, 370)$
- $767G = (1, 377)$
- $768G = (0, 375)$
- $769G = O$ (point at infinity)

If Alice wants to send to Bob the message $M$ which is encoded as the plaintext point $P_M = (443, 253) \in E_{751}(-1, 188)$. She must use Bob’s public key to encrypt it. Suppose that Bob’s secret key is $n_B = 85$, then his public key will be:

$$P_B = n_BG = 85(0, 376)$$

$$P_B = (671, 558)$$
Alice selects a random number $k = 113$ and uses Bob’s public key $P_B = (671, 558)$ to encrypt the message point into the ciphertext pair of points:

$$
P_C = [(kG), (P_M + kP_B)]
$$

$$
P_C = [113 \times (0, 376), (443, 253) + 113 \times (671, 558)]
$$

$$
P_C = [(34,633), (443, 253) + (47, 416)]
$$

$$
P_C = [(34,633), (217, 606)]
$$

Upon receiving the ciphertext pair of points, $P_C = [(34,633), (217, 606)]$, Bob uses his private key, $n_B = 85$, to compute the plaintext point, $P_M$, as follows

$$
(P_M + kP_B) - [n_B(kG)] = (217, 606) - [85(34,633)]
$$

$$
(P_M + kP_B) - [n_B(kG)] = (217, 606) - [(47, 416)]
$$

$$
(P_M + kP_B) - [n_B(kG)] = (217, 606) + [(47, -416)] \quad \text{(since } -P = (x_1, -y_1))
$$

$$
(P_M + kP_B) - [n_B(kG)] = (217, 606) + [(47, 335)] \quad \text{(since } -416 \equiv 335 \pmod{751})
$$

$$
(P_M + kP_B) - [n_B(kG)] = (443, 253)
$$

and then maps the plaintext point $P_M = (443, 253)$ back into the original plaintext message $M$.

---

**Security of ECC**

The cryptographic strength of elliptic curve encryption lies in the difficulty for a cryptanalyst to determine the secret random number $k$ from $kP$ and $P$ itself. The fastest method to solve this problem (known as the *elliptic curve logarithm problem*) is the Pollard $\rho$ factorization method [Sta99].

The computational complexity for breaking the elliptic curve cryptosystem, using the Pollard $\rho$ method, is $3.8 \times 10^{10}$ MIPS-years (i.e. millions of instructions per second times the required number of years) or an elliptic curve key size of only 150 bits [Sta99]. For comparison, the fastest method to break RSA, using the *General Number Field Sieve Method* to factor the composite integer $n$ into the two primes $p$ and $q$, requires $2 \times 10^8$ MIPS-years for a 768-bit RSA key and $3 \times 10^{11}$ MIPS-years with a RSA key of length 1024.

If the RSA key length is increased to 2048 bits, the General Number Field Sieve Method will need $3 \times 10^{20}$ MIPS-years to factor $n$ whereas increasing the elliptic curve key length to only 234 bits will impose a computational complexity of $1.6 \times 10^{28}$ MIPS-years (still with the Pollard $\rho$ method).