Chapter 10
Elliptic Curves in Cryptography

February 15, 2010

10

Elliptic Curves (ECs) can be used as an alternative to modular arithmetic in all applications based on the Discrete Logarithm (DL) problem.

The DL problem is:
Given $n,\ b,\ \alpha$; find x from $b = \alpha^x \ mod\ n$.

The EC equivalent is:
Given points $P,\ Q$ on an EC. Find N from $Q = NP$.

Here NP means "add the point P to itself N times". Clearly we need a definition of the meaning of "adding points". The EC equivalent of "$mod\ n$" is obtained by working over a finite field $GF(q)$; so that all points $P = (x,\ y)$ on the curve have $x,\ y \in\ GF(q)$. The EC used is a discrete set of points satisfying $y^2 + xy = x^3 + ax^2 + b$, with $q = 2^m$, so that $GF(q)$ has characteristic equal to two. Hasse's Theorem states that $Order(EC) = Number\ of\ points\ on\ the\ EC\ \approx\ q \pm 2\sqrt{q}$. The points on the EC form a group under the addition rule, and of course the order of any point divides the order of the group.

The fact that ECs use repeated addition (to provide multiplication) whereas in modular arithmetic we use repeated multiplication (to provide exponentiation) should, in principle, explain the advantages of using ECs - they should result in faster calculations. In fact this is only marginally so, because EC-addition is complex and involves multiplication (in $GF(q)$).

The real advantage of ECs in cryptography is that there are no known sub-exponential attacks on ECs as there are when modular arithmetic is used. These sub-exponential attacks rely on factorising over a factor base and no

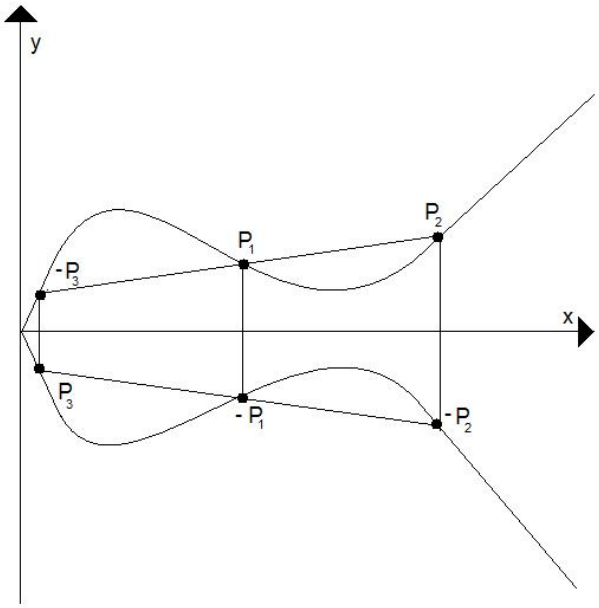
such concept exists in ECs. Therefore ECs, using numbers of a given size, are more secure than the corresponding modular arithmetic schemes, when applied to the DL problem. Alternatively, an EC-DL-based system can have the same security as a Modular Arithmetic DL - based system - *but with smaller numbers*, and so be much faster.

10.1 Elliptic Curves

(It is easiest to introduce ECs over real numbers before considering ECs over finite fields).

An EC over the real plane can be simplified to have equation $y^2 = x^3 + ax + b$. It lies to the right of a vertical line given by $x^3 + ax + b = 0$. It is mirrored in a horizontal line given by $y = 0$. Any straight line cuts the curve in three points (if we include "the point at infinity"$= \theta$ as a point, to handle vertical lines.)

Addition of points is defined by "The sum of any three points on the curve, on the same straight line, is zero". Therefore if P_1 and P_2 are two points on the curve, $P_3(= P_1 + P_2)$ is defined as the negative (or mirror image in $y = 0$) of the point at which the line (P_1P_2) cuts the curve again. The negative of a point is its mirror image in $y = 0$. $P + (-P) = \theta$, so in this sense θ is the group identity element.



The point $Q = 2P$ is defined similarly, but the line is now the tangent at P.

Clearly, given $P_1(= (x_1 y_1))$ $P_2(= (x_2 y_2))$ P_3's coordinates can be simply determined by algebra.

In the appendix an example is given of an EC, but this time it is over $GF(2^m)$ with $m = 4$ specifically. Moreover the Finite Field $GF(2^k)$ is represented in a peculiar way (see appendix) using an Optimal Normal Base (ONB) given by the irreducible, but non-primitive, polynomial $f(x) = x_4 + x_3 + x_2 + x + 1$. ONBs are not necessary for EC calculations over finite fields, but they make the calculations faster (if more obscure).

10.2 Sample Applications

(See Chapter 5 for Modular Arithmetic Equivalent)

1. Diffie-Hellman with ECs

A and B share an EC (conceptually of course) and a point P on it. They establish a new point Q on it which is a secret shared by them alone, as follows

A	**B**
Invents c (*integer*)	*Invents* d (*integer*)
Sends point cP *to* B	*Sends point* dP *to*A
	
A *forms* Q=c(dP)	B *forms* Q=d(cP)

$c,\ d$ are integers. The secret point Q can be used as a source of data, example: for a secret key - by merging the $x,\ y$ coordinate values of Q together using some agreed algorithm.

An attacker who sees the points $cP,\ dP$ in transit, and who knows the curve and P, still cannot find c or d (the DL problem). So the attacker cannot find Q.

10.3 D.S.A. with ECs

There exist a common EC and a base point P. The order of $P = n$.

10.3.1 DSA - Sign

Signatory's private key = d (integer)
Public key = dP =Q
Message = m

(a) Invert k (integer) and form $k^{-1}\ mod\ n$

(b) Form $R = kP$ ($R = (x,\ y)$ say)

(c) Convert x to integer z

(d) $r = z\ mod\ n$

(e) $s = k^{-1}(Hash(m) + dr)$

(f) Signature = $(r,\ s)$ two integers

10.3.2 EC-DSA-Validate

(a) Receive m and signature $(r,\ s)$

(b) $c = s^{-1} mod\ n$

(c) $u_1 = H(m).c \ mod \ n$, $u_2 = r.c \ mod \ n$

(d) Compute

$$\begin{aligned} \mathrm{R} &= \mathrm{u}_1 P + u_2 Q \\ &= \mathrm{u}_1 P + u_2 dP \\ &= (\mathrm{H(m)c+rcd})\mathrm{P} \\ &= \mathrm{s}^{-1}(H(m) + rd)P \\ &= \mathrm{kP} \end{aligned}$$

(e) If $R = (x, \ y)$ convert x to integer z

(f) $v = z \ mod \ n$

(g) Test if $r = v$, if yes then signature is correct.

10.4 (Shanks') Algorithm to Solve DL Problem in ECs

Suppose $S = xP$. How to find x?

Suppose $Order \ (P) \sim \ n$. Let $d = n^{\frac{1}{2}}$ and suppose $x = qd + r$ where $0 \leq q < d$ and $0 \leq r < d$.

Then we tabulate jP for $1 \leq j \leq d - 1$ and form $(S + (n - id)P)$ for i increasing from zero and we look for $(s + (n - id)P) = jP$ for some j in the table.

When this occurs it means that

$$\begin{aligned} \mathrm{S+(n\text{-}id)P} &= \mathrm{(n+(q\text{-}i)d+r)P} \\ &= \mathrm{((q\text{-}i)d + r)P} \\ Therefore \ \mathrm{q} &= \mathrm{i \ (since \ the \ table \ only \ contains \ jP \ with \ j \ less \ than \ d)} \\ and \ \mathrm{r} &= \mathrm{j} \end{aligned}$$

So x has been found, $x = qd + r$.

But this algorithm taken time $T \propto n^{\frac{1}{2}}$ or $log \ T = \frac{1}{2} \ log \ n$. (Compared with $log \ T = a(log \ n \ log \ log \ n)^{\frac{1}{2}}$ using a factor base.)

Therefore EC-DL problem is more secure for similarly sized n, than is the Modular Arithmetic DL problem.

Appendix X
Elliptic Curves Over $GF(2^m)$

(a) Curves: $y^2 + xy = x^3 + ax^2 + b$
For given $x,\ y$ has two roots $y_1,\ y_2$ with

$$\mathrm{y}_1 + y_2 = x \text{ i.e. } y_1 = x + y_2 \tag{0.1}$$

(b) Curve cut by $y = mx + c$ at
$m^2x^2 + [2mxc = 0, since\ characteristic = 2] + c^2 + mx^2 + cx = x^3 + ax^2 + b$
or $x^3 + x^2(m^2 + m + a) + cx + b + c^2 = 0$
Therefore $x_3 + x_2 + x_1 = m^2 + m + a$ or

$$\mathrm{x}_3 = m^2 + m + a + x_2 + x_1 \tag{0.2}$$

where $y = mx + c$ is a line linking $P_1(x_1y_1)$ and $P_2(x_2y_2)$
$y_3 = x_3 + (mx_3 + c)$ (to get other root, not on line see equation **??** above)
$y_3 = mx_3 + [mx_1 + y_1 = c] + x_3$
$y_3 = m(x_3 + x_1) + y_1 + x_3$

$$\mathrm{y}_3 = m(x_3 + x_2) + y_2 + x_3 \tag{0.3}$$

$$\text{Here m} = (\mathrm{y}_2 + y_1)/(x_2 + x_1) \tag{0.4}$$

But if $x_1 = x_2$.
$2y\frac{dy}{dx} + x\frac{dy}{dx} + y = 3x^2 + 2ax = x^2$
$x\frac{dy}{dx} + y = 3x^2 = x^2$

Therefore $\frac{dy}{dx} = \frac{x^2+y}{x}$, $(\frac{dy}{dx})_{x_1} = x_1 + \frac{y_1}{x_1}$

i.e. $$\mathrm{m}=\mathrm{x}_1 + y_1/x_1 \tag{0.5}$$

Then $$\mathrm{x}_3 = m^2 + m + a \tag{0.6}$$

$$\mathrm{y}_3 = (m+1)x_3 + mx_1 + y_1 = (m+1)x_3 + x_1^2 \tag{0.7}$$

To check this works:

$P_1 + P_2 \Rightarrow P_3$ as above. Test $P_3 + (-P_1) =?$
$P_3 + (-P_1) = (x_3,\ y_3) + (x_1,\ x_1 + y_1)$ (from equation **??**)
$m^* = \frac{y_3+x_1+y_1}{x_3+x_1} = \frac{(m+1)(x_3+x_1)}{x_3+x_1} = m + 1$ (using equation **??**)

$$\begin{array}{rrcll}
Therefore & \mathrm{x}_{P_3-P_1} & = & \mathrm{m}^{*^2} + m^* + a + x_3 + x_1 & \\
 & & = & \mathrm{m}^2 + m + a + x_3 + x_1 & \\
So & \mathrm{x}_{P_3-P_1} & = & \mathrm{x}_2 & \\
and & \mathrm{y}_{P_3-P_1} & = & \mathrm{m}^*_{x_2} + m^*_{x_3} + y_3 + x_2 & (equation\ \mathbf{??}) \\
 & & = & \mathrm{m}x_2 + mx_3 + y_3 + x_3 & \\
 & & = & \mathrm{y}_2 & \\
Therefore & \mathrm{P}_3 + (-P_1) & = & \mathrm{P}_2 & Correct.
\end{array}$$

Example Curve Curve is $y^2 + xy = x^3 + \alpha^3 x^2 + \alpha^6$

$\alpha^0 = 1111$	$\alpha = 1100$	$\alpha^2 = 0110$	$\alpha^3 = 0100$
$\alpha^4 = 0011$	$\alpha^5 = 1010$	$\alpha^6 = 0010$	$\alpha^7 = 0111$
$\alpha^8 = 1001$	$\alpha^9 = 1000$	$\alpha^{10} = 0101$	$\alpha^{11} = 1110$
$\alpha^{12} = 0001$	$\alpha^{13} = 1101$	$\alpha^{14} = 1011$	$\alpha^{15} = 1111$

This representation is based on an Optimal Normal Base (ONB) for $GF(2^4)$. An ONB allows faster calculations. For example, squaring is a right-rotation.

The points on the curve are:

$(0,\ \alpha^3)$	$(\alpha^3,\ \alpha^{13})$	$(\alpha^5,\ 0)$	$(\alpha^{13},\ \alpha^5)$	$(\alpha^4,\ \alpha^8)$	$(\alpha^{14},\ \alpha^2)$	$(\alpha^0,\ \alpha^{12})$
$(\alpha^3,\ \alpha^8)$	$(\alpha^5,\ \alpha^5)$	$(\alpha^{13},\ \alpha^7)$	$(\alpha^4,\ \alpha^5)$	$(\alpha^{14},\ \alpha^{13})$	$(\alpha^0,\ \alpha^{11})$	Point at infinity

0.0.1 Sample Calculation

Take $P = (1,\ \alpha^{11})$, then $2P$ is

$$\begin{aligned} \mathrm{x}_3 &= \mathrm{m}^2 + m + \alpha^3 \\ \mathrm{y}_3 &= \mathrm{x}_1^2 + (m+1)x_3 \ = \ 1 + (m+1)x_3 \\ \mathrm{m} &= 1+\alpha^4 \ = \ \alpha^{12} \\ \mathrm{x}_3 &= \alpha^{13} \\ \mathrm{y}_3 &= \alpha^7 \qquad 2P = (\alpha^{13},\ \alpha^7) \end{aligned}$$

and 3P=2P+P

$$\begin{aligned} \mathrm{x}_3 &= \mathrm{m}^2 + m + \alpha^3 + 1 + \alpha^{13} \\ \mathrm{y}_3 &= \mathrm{m}(\mathrm{x}_3 + 1) + \alpha^{11} + x_3 \\ \mathrm{m} &= (\mathrm{y}_2 + y_1)/(x_2 + x_1) \ = \ (\alpha^{11} + \alpha^7)/(1 + \alpha^{13}) \ = \ (\alpha^8)/(\alpha^6) \ = \\ \mathrm{x}_3 &= \alpha^4 \\ \mathrm{y}_3 &= \alpha^8 \qquad 3P = (\alpha^4,\ \alpha^8) \end{aligned}$$

Number of calculations involved are (XORs, Squarings ignored):

$$\begin{aligned} m &\Rightarrow \textit{One division} \\ x &\Rightarrow \textit{Nil} \\ y &\Rightarrow \textit{One multiplication} \end{aligned}$$

Remark The IEEE P1363 provides recommendations for the cryptographic use of ECs.