Date: Monday, September 24, 2002
Prof.: Dr Jean-Yves Chouinard

Design of Secure Computer Systems CSI4138/CEG4394
Notes on Elliptic Curve Cryptography

1 Elliptic Curve Cryptography

1.1 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 intersecting an elliptic curve, then 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 $y^2 = x^3 - 2x + 1$.

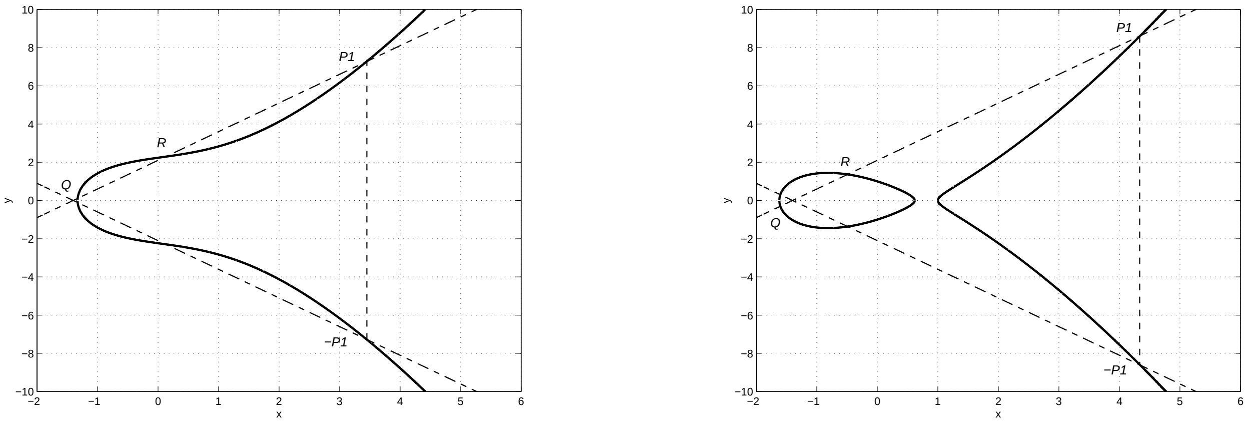

Figure 1: Elliptic curves $y^2 = x^3 + 2x + 5$ and $y^2 = x^3 - 2x + 1$.

1.2 Elliptic Curves over Galois Fields

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

$$4a^3 + 27b^2 \bmod p \neq 0$$

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 $b = 1$. We first verify that:

$$\begin{aligned}
4a^3 + 27b^2 \bmod p &= 4 \times 1^3 + 27 \times 1^2 \bmod 23 \\
4a^3 + 27b^2 \bmod p &= 4 + 27 \bmod 23 = 31 \bmod 23 \\
4a^3 + 27b^2 \bmod p &= 8 \neq 0
\end{aligned}$$

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

$x^2 \bmod p$	$(p - x)^2 \bmod p$	$=$
$1^2 \bmod 23$	$22^2 \bmod 23$	1
$2^2 \bmod 23$	$21^2 \bmod 23$	4
$3^2 \bmod 23$	$20^2 \bmod 23$	9
$4^2 \bmod 23$	$19^2 \bmod 23$	16
$5^2 \bmod 23$	$18^2 \bmod 23$	2
$6^2 \bmod 23$	$17^2 \bmod 23$	13
$7^2 \bmod 23$	$16^2 \bmod 23$	3
$8^2 \bmod 23$	$15^2 \bmod 23$	18
$9^2 \bmod 23$	$14^2 \bmod 23$	12
$10^2 \bmod 23$	$13^2 \bmod 23$	8
$11^2 \bmod 23$	$12^2 \bmod 23$	6

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

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

x	0	1	2	3	4	5	6	7	8	9	10	11
y^2	1	3	11	8	0	16	16	6	15	3	22	9
$y^2 \in \mathbf{Q}_{23}$?	yes	yes	no	yes	no	yes	yes	yes	no	yes	no	yes
y_1	1	7		10	0	4	4	11		7		3
y_2	22	16		13	0	19	19	12		16		20

x	12	13	14	15	16	17	18	19	20	21	22
y^2	16	3	22	10	19	9	9	2	17	14	22
$y^2 \in \mathbf{Q}_{23}$?	yes	yes	no	no	no	yes	yes	yes	no	no	no
y_1	4	7				3	3	5			
y_2	19	16				20	20	18			

The elliptic group $E_p(a,b) = E_{23}(1,1)$ thus include the points[1]:

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

Figure 2 shows a scatterplot of the elliptic group $E_p(a,b) = E_{23}(1,1)$.

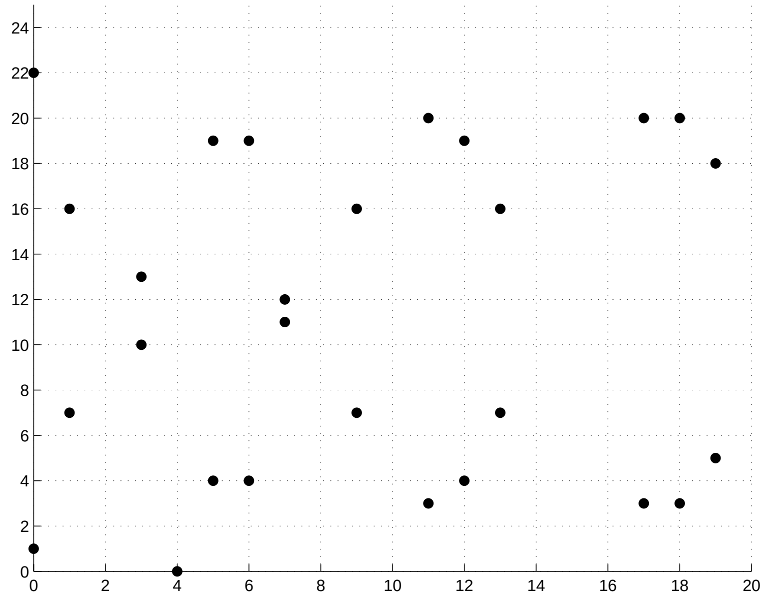

Figure 2: Scatterplot of elliptic group $E_p(a,b) = E_{23}(1,1)$.

[1]The elliptic group $E_{23}(1,1)$ also includes the additional point $(4,0)$, corresponding to the single value $y = 0$.

1.3 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 be 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 their sum $P + Q = (x_3, y_3)$ is given by:

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

   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 operation 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 λ, x_3 and y_3 are given by:

$$\begin{aligned} \lambda &= \frac{3x_1^2 + a}{2y_1} \bmod p = \frac{3 \times (3^2) + 1}{2 \times 10} \bmod 23 = \frac{5}{20} \bmod 23 = 4^{-1} \bmod 23 = 6 \\ x_3 &= \lambda^2 - x_1 - x_2 \bmod p = 6^2 - 3 - 3 \bmod 23 = 30 \bmod 23 = 7 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \bmod p = 6 \times (3 - 7) - 10 \bmod 23 = -34 \bmod 23 = 12 \end{aligned}$$

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

The multiplication kP is obtained by repeating the elliptic curve addition operation k times by following the same additive rules.

k	$\lambda = \frac{y_2-y_1}{x_2-x_1}$ (if $P \neq Q$) or $\lambda = \frac{3x_1^2+a}{2y_1}$ if $P = Q$	x_3 $\lambda^2 - x_1 - x_2 \bmod 23$	y_3 $\lambda(x_1 - x_3) - y_1 \bmod 23$	kP (x_3, y_3)
1				(3,10)
2	6	7	12	(7,12)
3	12	19	5	(19,5)
4	4	17	3	(17,3)
5	11	9	19	(9,16)
6	1	12	4	(12,4)
7	7	11	3	(11,3)
8	2	13	16	(13,16)
9	19	0	1	(0,1)
10	3	6	4	(6,4)
11	21	18	20	(18,20)
12	16	5	4	(5,4)
13	20	1	7	(1,7)
14	13	4	0	(4,0)
15	13	1	16	(1,16)
16	20	5	19	(5,19)
17	16	18	3	(18,3)
18	21	6	19	(6,19)
19	3	0	22	(0,22)
20	19	13	7	(13,7)
21	2	11	20	(11,20)
22	7	12	19	(12,19)
23	1	9	7	(9,7)
24	11	17	20	(17,20)
25	4	19	18	(19,18)
26	12	7	11	(7,11)
27	6	3	13	(3,13)

1.4 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 for which $nG = O$ is a very large prime number. The elliptic group $E_p(a,b)$ and the generator point G are made public.

Each user select a private key, $n_A < n$ and compute the public key P_A as: $P_A = n_A G$. To encrypt the message point P_M for Bob (B), Alice (A) choses a random integer k and compute 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, $(P_M + kP_B)$:

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

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 point, i.e. $(P_M + kP_B)$, and hence retrieve the plaintext information P_M.

Example*(Elliptic curve encryption):*

Consider the following elliptic curve:

$$\begin{aligned} y^2 &= x^3 + ax + b \bmod p \\ y^2 &= x^3 - x + 188 \bmod 751 \end{aligned}$$

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

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

$G = (0,376)$	$2G = (1,376)$	$3G = (750,375)$	$4G = (2,373)$
$5G = (188,657)$	$6G = (6,390)$	$7G = (667,571)$	$8G = (121,39)$
$9G = (582,736)$	$10G = (57,332)$	$\dots$	$761G = (565,312)$
$762G = (328,569)$	$763G = (677,185)$	$764G = (196,681)$	$765G = (417,320)$
$766G = (3,370)$	$767G = (1,377)$	$768G = (0,375)$	$769G = O$(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 public key to encrypt it. Suppose that Bob secret key is $n_B = 85$, then his public key will be:

$$\begin{aligned} P_B &= n_B G = 85(0, 376) \\ P_B &= (671, 558) \end{aligned}$$

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:

$$\begin{aligned} P_C &= [(kG), (P_M + kP_B)] \\ P_C &= [113 \times (0, 376), (443, 253) + 113 \times (671, 558)] \\ P_C &= [(34, 633), (443, 253) + (47, 416)] \\ P_C &= [(34, 633), (217, 606)] \end{aligned}$$

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

$$\begin{aligned} (P_M + kP_B) - [n_B(kG)] &= (217, 606) - [85(34, 633)] \\ (P_M + kP_B) - [n_B(kG)] &= (217, 606) - [(47, 416)] \\ (P_M + kP_B) - [n_B(kG)] &= (217, 606) + [(47, -416)] \qquad (\text{since } -P = (x_1, -y_1)) \\ (P_M + kP_B) - [n_B(kG)] &= (217, 606) + [(47, 335)] \qquad (\text{since } -416 \equiv 335 \pmod{751}) \\ (P_M + kP_B) - [n_B(kG)] &= (443, 253) \end{aligned}$$

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

1.5 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 ρ factorization method [Sta99].

The computational complexity for breaking the elliptic curve cryptosystem, using the Pollard ρ method, is 3.8×10^{10} MIPS-years (i.e. millions of instructions per second times the required number of years) for 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 interger n into the two primes p and q, requires 2×10^8 MIPS-years for a 768-bit RSA key and 3×10^{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 3×10^{20} MIPS-years to factor n whereas increasing the elliptic curve key length to only 234 bits will impose a computational complexity of 1.6×10^{28} MIPS-years (still with the Pollard ρ method).

References

[Sta99] W. Stallings. *Cryptography and Network Security: Principles and Practice*. Prentice-Hall, Upper Saddle River, New-Jersey, second edition, 1999.