Elliptic Curves Signature

Giulia Mauri

Politecnico di Milano

email: *giulia.mauri@polimi.it*
website: *http://home.deib.polimi.it/gmauri*

May 27, 2015

Overview

1. Elliptic Curves Signature
   - ElGamal Digital Signature
   - ECDSA

Elliptic Curve

Definition (Elliptic Curve)

An elliptic curve E is the graph of an equation:

$$E : y^2 = x^3 + ax^2 + bx + c$$

Definition (Addition Law)

Let E given by $y^2 = x^3 + bx + c$ and let $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$.
Then $P_1 + P_2 = P_3 = (x_3, y_3)$, where:

$x_3 = m^2 - x_1 - x_2$

$y_3 = m(x_1 - x_3) - y_1$

$$m = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1} & \text{if } P_1 \neq P_2 \\ (3x_1^2 + b)(2y_1)^{-1} & \text{if } P_1 = P_2 \end{cases}$$

If the slope m is infinite, then $P_3 = \infty$. There is one additional law: $\infty + P = P$ for all points P.

ElGamal Digital Signature

Alice wants to sign a document. Alice first must establish a public key. She chooses the curve E, the prime p, the number of points n, and the points A and $B = aA$. While Alice keeps secret the integer a.

To sign a document m, Alice does the following:

1. Computes $R = kA = (x, y)$, where k is a random integer with $1 \leq k < n$ and $gcd(k, n) = 1$
2. Computes $s \equiv k^{-1}(m - ax) \pmod{n}$
3. Sends the signed message (m, R, s) to Bob.

Bob verifies the signature as follows:

1. Computes $V_1 = xB + sR$ and $V_2 = mA$
2. Declares the signature valid if $V_1 = V_2$

Exercise 1

Exercise

Alice uses the following ElGamal signature with elliptic curves. Alice chooses the curve:

$$E : y^2 \equiv x^3 + 3 \pmod{31}$$

The number $p = 31$ *is prime. Alice computes the number of points* n *which belong to the curve and obtain* $n = 43$*. On the curve* E *she chooses the point* $A = (1, 2)$ *and the secret number* $a = 18$*. She then computes the position of the point* $B = aA$ *and obtains:*

$$B = aA = (17, 24)$$

Alice publishes the curve E*, the number* p *and the position of the points* A *and* B*. The number* a *is kept secret.*

Exercise 1

Exercise

1. *Alice wants to send the message* $m_1 = 7$ *and chooses the random number* $k = 3$. *Compute Alice's signature.*
2. *Verify the signature.*
3. *Alice, then, signs a second message* $m_2 = 13$ *and uses the same nonce as before, obtaining* $R_2 = (22, 24), s_2 = 30$. *Bob computes the nonce.*

Exercise 1

Solution

Alice must compute: $R = kA = 3 \cdot (1,2) = (1,2) + (1,2) + (1,2)$
We first compute $2(1,2)$*, obtaining:* $m = 3 \cdot 4^{-1} \bmod 31 = 3 \cdot 8 = 24$
To compute the inverse of 4 modulo 31 we can use the extended Euclidean algorithm. By solving the equations for x_3 *e* y_3 *we obtain:*

$$\begin{aligned} x_3 &= m^2 - x_1 - x_2 = 24^2 - 2 \cdot 1 \mod 31 = 16 \\ y_3 &= m(x_1 - x_3) - y_1 = 24(1 - 16) - 2 = 10 \end{aligned}$$

We then sum $(1,2) + (16,10)$ *and obtain:*

$$m = 8 \cdot 15^{-1} \mod 31 = 8 \cdot (-2) = 15$$
$$x_3 = 15^2 - 1 - 16 \mod 31 = 22$$
$$y_3 = 15 \cdot (1 - 22) - 2 \mod 31 = 24$$

Therefore $R = (22, 24)$.

Exercise 1

Solution

We compute s:

$$s = k^{-1}(m - ax_R) = 3^{-1}(7 - 18 \cdot 22) \mod 43 =$$
$$= 29 \cdot (-389) \mod 43 = 28$$

Alice publishes the message m and the signature (m, R, s). *Then, we verify the signature:*

$$V_1 = x_R B + sR = 22 \cdot (17, 24) + 28 \cdot (22, 24)$$
$$= (9, 22) + (16, 21) = (25, 29)$$
$$V_2 = mA = 7 \cdot (1, 2) = (25, 29)$$

The signature is verified.

Exercise 1

Solution

We compute the nonce as follows:

$$\begin{aligned} s_1 k - m_1 = -a x_R = s_2 k - m_2 \pmod{n} \\ (s_1 - s_2)k = (m_1 - m_2) \pmod{n} \\ (28 - 30)k = (7 - 13) \pmod{43} \\ 41k = 37 \pmod{43} \\ k = 37 \cdot 41^{-1} \pmod{43} = 37 \cdot 21 = 3 \end{aligned}$$

ECDSA

Alice wants to sign a document m, which is an integer. Alice chooses the curve E, the prime p, a large prime factor q ($qA = \infty$) of n (number of points), and the points A and $B = aA$. Alice's secret parameter is the integer a.

Alice does the following:

1. Computes $R = kA = (x_R, y_R)$, where k is a random integer with $1 \leq k < q$
2. Computes $s \equiv k^{-1}(m + ax_R) \pmod{q}$
3. Sends the signed message (m, R, s) to Bob.

Bob verifies the signature as follows:

1. Computes $u_1 \equiv s^{-1}m \pmod{q}$ and $u_2 \equiv s^{-1}x_R \pmod{q}$
2. Computes $V = u_1 A + u_2 B$
3. Declares the signature valid if $V = R$.

Exercise 2

Exercise

The parameters of ECDSA are given by the curve $E : y^2 = x^3 + 2x + 2 \bmod 17$, *the point* $A = (5, 1)$ *of order* $q = 19$ *and Bob's private* $a = 10$. *Show the process of signing (Bob) and verification (Alice) for the following hash values and the nonces* k:

a $m = 12, k = 11$

b $m = 4, k = 13$

c $m = 9, k = 8$

Exercise 2

Solution

a

$$R = kA = 11 * (5, 1) = (13, 10)$$

$$s = (m + ax_R)k^{-1} = (12 + 10 \cdot 13)11^{-1} \bmod 19 = 6$$

$$u_1 = ms^{-1} = 12 \cdot 6^{-1} \bmod 19 = 2$$

$$u_2 = x_r \cdot s^{-1} = 13 \cdot 6^{-1} \bmod 19 = 18$$

$$V = u_1 A + u_2 B = 2(5, 1) + 18(7, 11) = (13, 10)$$

Exercise 2

Solution

b

$$R = kA = 13 * (5, 1) = (16, 4)$$

$$s = (m + ax_R)k^{-1} = (4 + 10 \cdot 16)13^{-1} \bmod 19 = 17$$

$$u_1 = ms^{-1} = 4 \cdot 17^{-1} \bmod 19 = 17$$

$$u_2 = x_r \cdot s^{-1} = 16 \cdot 17^{-1} \bmod 19 = 11$$

$$V = u_1 A + u_2 B = 17(5, 1) + 11(7, 11) = (16, 4)$$

Exercise 2

Solution

c

$$R = kA = 8 * (5,1) = (13,7)$$

$$s = (m + ax_R)k^{-1} = (9 + 10 \cdot 13)8^{-1} \bmod 19 = 15$$

$$u_1 = ms^{-1} = 9 \cdot 15^{-1} \bmod 19 = 12$$

$$u_2 = x_r \cdot s^{-1} = 13 \cdot 15^{-1} \bmod 19 = 11$$

$$V = u_1 A + u_2 B = 12(5,1) + 11(7,11) = (13,7)$$

Exercise 3

Exercise

Alice uses the DSA signature scheme on the elliptic curve $E : y^2 \equiv x^3 + 3x + 8 \mod 23$. *The curve* E *has* 29 *points. Alice chooses the base point* $A = (0, 10)$, *the secret* $a = 5$ *and computes* $B = aA$. *Then she signs the message* $m_1 = 3$ *using the nonce* $k = 2$.

(a) Verify if A *satisfies the conditions required by DSA signature.*

(b) Compute B.

(c) Sign m_1

(d) Verify the signature obtained in (c)

Exercise 3

Solution

(a) The order of A must be prime. In this case the number of points is prime, therefore all the points have order q.
(b) B=aA = 5(0,10) = 2(0,10)+2(0,10)+(0,10) = (1,14)+(1,14)+(0,10) =(16,14)+(0,10) = (20,8).
(c)

$$R = kA = 2A = 2(0,10) = (1,14)$$
$$s \equiv k^{-1}(m + ax_R) = 15(3 + 5 \cdot 1) = 4 \pmod{29}$$

(d)

$$u_1 \equiv s^{-1}m = 22 \cdot 3 = 8 \pmod{17}$$
$$u_2 \equiv s^{-1}x_R = 22 \cdot 1 = 22 \pmod{17}$$
$$V = u_1 A + u_2 B = 8A + 22B =$$
$$= 8(0,10) + 22(20,8) = (1,14)$$

Exercise 4

Exercise

Consider the elliptic curve $E : y^2 \equiv x^3 + 3 \pmod 7$*, with 13 points. Alice publishes the curve and the points* $A = (1, 2)$ *and* $B = aA = (2, 2)$*. Then, Alice signs the messages* $m_1 = 2$ *and* $m_2 = 3$ *using the DSA signature and obtains:*

$$sig(m_1, k_1) = (x_{R,1}, s_1) = (3, 10)$$

$$sig(m_2, k_2) = (x_{R,2}, s_2) = (3, 5)$$

1. *List all the points of curve E*
2. *Verify the signature of message* m_1
3. *Using the repeated nonce, compute* k_1
4. *Compute the secret number a*

Exercise 4

Solution

1

x	$y^2 \equiv a$	$a^{\frac{p-1}{2}}$	$y \equiv a^{\frac{p+1}{4}}$
0	3	-1	–
1	4	1	± 2
2	4	1	± 2
3	2	1	± 3
4	4	1	± 2
5	2	1	± 3
6	2	1	± 3
∞	–	–	∞

Exercise 4

Solution

2

$$u = s^{-1}m \bmod 13 = 8$$

$$v = s^{-1}x_R \bmod 13 = 12$$

$$V = 8A + 12B = 8A - B$$

$Compute\ 2A = 2(1,2)$

$$m = 3 \cdot 4^{-1} \bmod 7 = 6$$

$$x_{2,A} = 36 - 2 \bmod 7 = 6$$

$$y_{2,A} = 6(1-6) - 2 \bmod 7 = 3$$

Exercise 4

Solution

2 *Compute* $4A = 2(6,3)$

$$m = 108 \cdot 6^{-1} \bmod 7 = 4$$

$$x_{4,A} = 16 - 12 \bmod 7 = 4$$

$$y_{4,A} = 4(6-4) - 3 \bmod 7 = 5$$

Compute $8A = 2(4,5)$

$$m = 48 \cdot 10^{-1} \bmod 7 = 2$$

$$x_{8,A} = 4 - 8 \bmod 7 = 3$$

$$y_{8,A} = 2(4-3) - 5 \bmod 7 = 4$$

Exercise 4

Solution

2 *Compute* $V = (3,4) + (2,5)$

$$m = (5-4)(2-3)^{-1} \bmod 7 = 6$$

$$x_V = 36 - 3 - 2 \bmod 7 = 3$$

$$y_V = 6(3-2) - 3 \bmod 7 = 3$$

Since $x_V = x_R$*, the signature is verified.*

3

$$s_1 k - m_1 \equiv a x_R \equiv s_2 k - m_2 \pmod{13}$$

$$(s_1 - s_2)k \equiv m_1 - m_2 \pmod{13}$$

$$5k \equiv 12 \pmod{13}$$

$$k \equiv 12 \cdot 5^{-1} \equiv 5 \pmod{13}$$

Exercise 4

Solution

4

$$s_1 k - m_1 \equiv a x_R \pmod{13}$$

$$a \equiv (x_R)^{-1}(s_1 k - m_1) \equiv 9 \cdot 48 \equiv 3 \pmod{13}$$

Exercise 5

Exercise

Alice uses the DSA signature scheme on the elliptic curve $E : y^2 \equiv x^3 + 2x + 6 \mod 7$. *The curve* E *has* 11 *points. Alice chooses the base point* $A = (1, 3)$, *the secret* $a = 4$ *and computes* $B = aA$. *Then she signs the message* $m_1 = 3$ *using the nonce* $k = 6$.

1. *Verify whether* A *satisfies the conditions required by DSA signature.*
2. *Compute* B.
3. *Sign* m_1.
4. *Verify the signature obtained in 3.*
5. *Alice signs the message* $m' = 4$ *and publishes* $sig(m_2) = [R_2, s_2, m_2] = [(4, 6), 7, 4]$. *Which mistake did she do? How can it be exploited by an attacker to find the secret key* a*?*

Exercise 5

Solution

1 *The order of A must be prime. In this case the number of points is prime, therefore all the points have order q.*

2

$$B = aA = 4(1,3) = 2(1,3) + 2(1,3) = (2,2) + (2,2) = (3,5)$$

3 *Signature:*

$$R = kA = 6A = 4(1,3) + 2(1,3) = (3,5) + (2,2) = (4,6)$$
$$s \equiv k^{-1}(m + ax_R) = 2(3 + 4 \cdot 4) = 5 \pmod{11}$$

Exercise 5

Solution

4 *Verification:*

$$u_1 \equiv s^{-1}m = 9 \cdot 3 = 5 \pmod{11}$$
$$u_2 \equiv s^{-1}x_R = 9 \cdot 4 = 3 \pmod{11}$$
$$V = u_1 A + u_2 B = 5A + 3B =$$
$$= 5(1,3) + 3(3,5) = (4,6)$$

Since $V = R$, the signature is verified.

Exercise 5

Solution

5 *Alice used the same k twice,so we can write the following equation:*

$$s_1 k - m_1 \equiv a x_R \equiv s_2 k - m_2 \pmod q$$
$$(s_1 - s_2) k \equiv m_1 - m_2 \pmod q$$
$$(5 - 7) k \equiv 3 - 4 \mod 11$$
$$k = 6$$

Now we substitute the value of k in the equation $sk - m \equiv a x_R$ and obtain:

$$a \equiv x_R^{-1}(sk - m) \pmod q$$
$$a \equiv 4^{-1}(5 \cdot 6 - 3) \equiv 4 \pmod{11}$$