Exercices : elliptic curves

Invalid curve attacks

We present classical attacks on static Diffie-Hellman based protocols over elliptic curves.

Attack against Weierstrass curves

Let $E : y^2 = x^3+ax+b$ be an elliptic curve in reduced Weierstrass form, defined over $\mathbb{F}_q$ in characteristic $p > 3$, such that the ECDLP is difficult on E.
In this attack, you are given a device that, given a point P, returns the point $s\,P$ where s is a secret integer.

1. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points of E. Give the coordinates of $P_3 = P_1 + P_2$, by distinguishing between $P_1 = P_2$, $P_1 = -P_2$ and $P_1 \neq \pm P_2$.
   How are the parameters a and b related to these coordinates ?
2. Let $P_0 = (x_0, y_0) \in (\mathbb{F}_q)^2$ and $b' = y_0^2 - x_0^3 - ax_0$. Show that P_0 belongs to the elliptic curve $E' : y^2 = x^3 + ax + b'$.
3. Assume that the provided device does not verify that the input values are points on E. What will be the output of a request with input P_0 ?
4. Give an attack that allows to recover the secret s with a polynomial numbers of calls to the device. Propose a simple countermeasure.
5. Application. The elliptic curve $E : y^2 = x^3 - 3x + 73$ defined over $\mathbb{Z}/199\mathbb{Z}$ admits 197 points. For the input $P = (183, 117)$, the device returns $Q = (99, 36)$.
   (a) Show that the point P is on the curve $E' : y^2 = x^3 - 3x + 26$ (defined over $\mathbb{Z}/199\mathbb{Z}$).
   (b) Easy computations give $\#E' = 210$, $105\,Q = (101, 0)$, $70\,Q = 70\,P = (136, 149)$, $42\,Q = -84\,P = (173, 144)$, and $30\,Q = \mathcal{O} \neq 30\,P$.
   Recover the value of s.

Attack against the Montgomery ladder

We have seen during the lectures that it is possible to devise a Diffie-Hellman protocol involving only x-coordinates. Using the Montgomery ladder, it is also possible to compute the x-coordinate of $k\,P$ with a fast exponentiation algorithm, without using the y-coordinaites.

We give some formulae. Let P, Q be two points of the curve E with equation $y^2 = x^3 + ax + b$. It is possible to get an expression of $x(P + Q)$ knowing only $x(P)$, $x(Q)$ and $x(P - Q)$:

$$x(P+Q) = f(x(P), x(Q), x(P-Q)) = \frac{-4b(x(P)+x(Q)) + (x(P)x(Q)-a)^2}{x(P-Q)(x(P)-x(Q))^2} \quad \text{if } P \neq \pm Q$$

$$x(2P) = g(x(P)) = \frac{(x(P)^2-a)^2 - 8bx(P)}{4(x(P)^3+ax(P)+b)} \quad \text{if } P \neq -P$$

Consider the following algorithm :

Input : $x = x(P)$, $k = (k_l, \ldots, k_0)_2$
$x_0 \leftarrow x$; $x_1 \leftarrow g(x)$
for $i = l-1$ down to 0 **do**
  if $k_i = 0$ **then**
    $x_1 \leftarrow f(x_1, x_0, x)$; $x_0 \leftarrow g(x_0)$
  else
    $x_0 \leftarrow f(x_1, x_0, x)$; $x_1 \leftarrow g(x_1)$
return x_0

1. Show that the output of the algorithm is the abscissa of $k\,P$.
2. Explain why the previous attack cannot be applied directly when this algorithm is used.

Let $c \in \mathbb{F}_q$ be an element which is not a square. We consider the curve E_c of equation $cy^2 = x^3 + ax + b$. We can then show that for all $x \in \mathbb{F}_q$,

— either $x^3 + ax + b$ is a square in $\mathbb{F}_q$, and then there exists $y \in \mathbb{F}_q$ such that (x, y) belongs to E

— or $x^3 + ax + b$ is not a square in $\mathbb{F}_q$, and then $\frac{1}{c}(x^3 + ax + b)$ is a square, and thus there exists $y \in \mathbb{F}_q$ such that (x, y) belongs to E_c.

3. We now suppose that our device uses the previously described algorithm and that it does not check the inputs. What is the output when the input is an element $x \in \mathbb{F}_q$ which is not the x-coordinate of a point in $E(\mathbb{F}_q)$?
4. Assume in this question that E is "*twist-insecure*", i.e. the cardinality of the curve E_c does not have small prime factors. Devise an attack that allows to recover information on s.
5. (Bonus) With the above property, show that $\#E_c = 2q + 2 - \#E$.
   Is the `brainpoolP256r1` curve "twist-secure" ? And the `secp256k1` curve, used in the Bitcoin protocol ?

Attacks against Edwards curves

The elliptic curve is now given in Edwards form $Ed : ax^2 + y^2 = 1 + dx^2y^2$ with a and d two distinct elements of $\mathbb{F}_q^*$. We recall the addition law for Edwards coordinates :

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

1. Assume now that the device uses the above addition law over Ed, but does not verify that the input are points on E_d. Is it possible to apply directly the attack of the question 4 ?
2. Let $P_0 = (0, y_0) \in (\mathbb{F}_q)^2$. Show that the output returned by the device for the input P_0 is $(0, y_0^s)$. Deduce an attack that allows to recover s.
3. Application.
   The curve Ed defined over $\mathbb{F}_{47}$ admits 53 points. On the input $(0, 40)$, the device returns $(0, 38)$. The goal is to apply the previous attack in order to recover s.
   (a) Knowing that $38^{23} = 40^{23} = -1$ [47], find the value of s modulo 2.
   (b) Use baby-step giant-step to recover s modulo 23. You can use the following computations : $38^2 = 34$ [47], $40^2 = 2$ [47] and $2^{-5} = 25 \bmod 47$.
   (c) Conclude.