Advanced Cryptology - Final Exam - (3 h)

Lecture notes allowed. No computer, cellphone off.

Problem: invalid curve attacks

Part 1

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve in short Weierstrass form defined over a finite field $\mathbb{F}_q$ of characteristic > 3, and such that the discrete logarithm problem on $E(\mathbb{F}_q)$ is difficult. You are given access to a device that given a point P, outputs the point $[s]P$ where s is a secret integer.

1. Given two affine points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, give the coordinates of $P_3 = P_1 + P_2$, distinguishing the cases $P_1 = P_2$, $P_1 = -P_2$ and $P_1 \neq \pm P_2$. How are the parameters a and b related to those 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 device does not check that its inputs are points on E. What will be the result of a query with input P_0?

4. Come up with an attack that recovers s using polynomially many queries to the device, and propose a simple countermeasure.

5. Application. The curve $E : y^2 = x^3 - 3x + 73$, defined over $\mathbb{F}_{199}$, has 197 rational points. On input $P = (183, 117)$, the device ouputs $Q = (99, 36)$. Some quick computations yield $117^2 - 183^3 + 3 \times 183 = 26\ [199]$, $\#(E' : y^2 = x^3 - 3x + 26) = 210$, $[105]Q = (101, 0)$, $[70]Q = 70[P] = (136, 149)$, $[42]Q = -[84]P = (173, 144)$, and $[30]Q = \mathcal{O} \neq [30]P$. Find s.

Part 2

For several reasons (mainly efficiency and protection against side-channel attacks), it has been proposed to use x-only multiplication algorithms.

6. Let $P \in E(\mathbb{F}_q)$ and $k \in \mathbb{Z}$. Show that $x([k]P)$ only depends of $x(P)$ (and not of $y(P)$). Come up with a Diffie-Hellman key exchange protocol using only x-coordinates.

7. Let P, Q be two points on E. Explain why it is possible to compute $x(P + Q)$ knowing only $x(P)$, $x(Q)$ and $x(P - Q)$.

8. The explicit formula is

$$x(P + Q) = f(x(P), x(Q), x(P - Q)) = \frac{-4b(x(P) + x(Q)) + (x(P)x(Q) - a)^2}{x(P - Q)(x(P) - x(Q))^2}.$$

Furthermore, $x(2P) = g(x(P)) = \dfrac{(x(P)^2 - a)^2 - 8bx(P)}{4(x(P)^3 + ax(P) + b)}$. We consider the following algorithm:

Input : $x = x(P)$, $k = (k_l, \dots, k_0)_2$
$x_0 \leftarrow x$; $x_1 = g(x)$
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

Prove that it ouputs $x([k]P)$.

9. Let $c \in \mathbb{F}_q$ be a non-square. We consider the curve E_c of equation $cy^2 = x^3 + ax + b$. Show that E_c is isomorphic to a quadratic twist of E. Recall the relationship between the cardinality of E and of its twist.

10. Show that for all $x \in \mathbb{F}_q$, there exists $y \in \mathbb{F}_q$ such that the point (x, y) belongs either to E or to E_c.

11. Assume that our device now uses the above x-only multiplication algorithm but still does not check its inputs. What is its ouput when queried with an element $x \in \mathbb{F}_q$ which is not the abscissa of a point of $E(\mathbb{F}_q)$?

12. Assume furthermore that E is *twist-insecure*, i.e. that the cardinality of its quadratic twist over $\mathbb{F}_q$ is smooth. Come up with an attack that recovers s.

Part 3

The elliptic curve is now given in twisted Edwards form: $Ed : ax^2 + y^2 = 1 + dx^2y^2$ where a and d are two distinct, non-zero elements of $\mathbb{F}_q$, a is a square and d is not a square in $\mathbb{F}_q$. The addition law is given by

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

We will admit that this formula indeed defines the elliptic curve groupe law (with neutral element $(0, 1)$) and that it is complete, i.e. the denominators never vanish.

13. Show that the only singular points of Ed are its points at infinity.

14. Assume our device now uses Ed and the above formula, but still does not check that its inputs are points on the curve. Is it possible to adapt directly the attack of question 4?

15. Let $P_0 = (0, y_0) \in (\mathbb{F}_q)^2$. Show that the result of a query to the device with input P_0 is $(0, y_0^s)$. Use this fact to propose an attack that recovers s.

16. Application.
The curve Ed defined over $\mathbb{F}_{47}$ has 53 rational points. On input $(0, 40)$, the device outputs $(0, 38)$. The goal is to apply the previous attack to recover s.

    (a) Knowing that $38^{23} = 40^{23} = -1$ [47] deduce the value of s modulo 2

(b) Use baby-step-giant-step to recover s modulo 23 knowing that $38^2 = 34$ [47], $40^2 = 2$ [47] and $2^{-5} = 25 \bmod 47$.

(c) Conclude.

Exercise 1.

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$.

1. Devise a point counting algorithm (i.e. an algorithm that computes $\#E(\mathbb{F}_q)$) and whose complexity is in $O(q)$ operations in $\mathbb{F}_q$.

2. Assume that the cardinality of $E(\mathbb{F}_q)$ is a prime number. Devise a (probabilistic) point counting algorithm whose complexity is in $O(q^{1/2})$ operations in $\mathbb{F}_q$.

3. Assume that the cardinality of $E(\mathbb{F}_q)$ is a prime number. Devise a (probabilistic) point counting algorithm whose complexity is in $O(q^{1/4})$ operations in $\mathbb{F}_q$ (hint: think baby-step giant-step). Can it be adapted to the case where $E(\mathbb{F}_q)$ is only assumed to be cyclic?

4. Assuming that E is a random ordinary curve, what is currently the best known algorithm for point counting on E? Give its complexity.

Exercise 2.

Let E be an elliptic curve defined over the finite field $\mathbb{F}_q$ and let n be a prime number such that $n^2 | \#E(\mathbb{F}_q)$ and $n \neq \mathrm{char}(\mathbb{F}_q)$.

1. Assume that $n \nmid q-1$. Explain why $E(\mathbb{F}_q)$ has points of order (exactly) n^2 and why $E(\mathbb{F}_q)[n] \simeq \mathbb{Z}/n\mathbb{Z}$.

We assume for the remainder of the exercise that $n|q-1$ and $E(\mathbb{F}_q)[n] \simeq \mathbb{Z}/n\mathbb{Z}$ (so that $E(\mathbb{F}_q)[n^2] \simeq \mathbb{Z}/n^2\mathbb{Z}$). The goal is to show that E is isogenous to a curve whose whole n-torsion is rational.

2. Let ϕ be the unique (up to $\mathbb{F}_q$-isomorphisms) separable isogeny of kernel $E(\mathbb{F}_q)[n]$ and $E' = E/E(\mathbb{F}_q)[n]$ its target curve. What is the degree of ϕ?

3. Let $P \in E(\mathbb{F}_q)$ be a point of order (exactly) n^2. Show that $Q = \phi(P)$ is a point of $E'(\mathbb{F}_q)$ of order n.

4. Let $\hat{\phi} : E' \to E$ be the dual isogeny of ϕ. Prove that $\hat{\phi}(Q) \neq O_E$ and deduce that $\ker(\hat{\phi}) \cap \langle Q \rangle = O_{E'}$.

5. We consider the linear transformation $\Phi_{q,n}$ of $E'[n]$ induced by the Frobenius endomorphism Φ_q of E'. Prove that $\langle Q \rangle$ and $\ker \hat{\phi}$ are two distinct eigenspaces of $\Phi_{q,n}$ and give the eigenvalue corresponding to $\langle Q \rangle$. Is $\Phi_{q,n}$ diagonalizable?

6. Show that the determinant of $\Phi_{q,n}$ is 1. Deduce that the Frobenius endomorphism induces the identity on $E'[n]$. What does this imply on $E'[n]$?

7. Application. If q is equal to a prime power p^{2d} (with $p \neq 2$), then the elliptic curves defined over $\mathbb{F}_q$ that admit an equation in Scholten form

$$y^2 = ax^3 + bx^2 + b^{p^d}x + a^{p^d}$$

are subject to the Weil descent attack on the discrete logarithm problem, which is slightly more efficient than Pollard-rho. Curves in Scholten form always have zero or three non-trivial 2-torsion points, and every elliptic curve having three non-trivial 2-torsion points can be put in Scholten form. Explain how this attack can be generalized to every curve whose cardinality is dividable by 4.