ECC Summer School – Exercices

Damien Robert

2015-09-25

1 Cryptography

Implement public key encryption and signature with elliptic curves:

El Gamal encryption :

- Alice has a secret key $a \in \mathbb{Z}/\ell\mathbb{Z}$ and public key $(P, aP) \in E(\mathbb{F}_p)^2$, where ℓ is a large prime dividing the order of $E/\mathbb{F}_p$, and P is of order ℓ. (To generate such a P take a random $P_0 \in E(\mathbb{F}_p)$ and set $P = \frac{\#E(\mathbb{F}_p)}{\ell} P_0$. Check that $P \neq 0_E$!)
- Bob wants to send $m \in E(\mathbb{F}_p)$ encrypted to Alice.
- Bob takes a random $b \in \mathbb{Z}/\ell\mathbb{Z}$ and send

$$u_1 = baP + m, u_2 = bP$$

- Alice recovers $m = u_1 - au_2$.

Signature (ECDSA, with some details skipped) :

- Alice has secret key a and public key (P, aP) as before;
- Signing $m \in \mathbb{Z}/\ell\mathbb{Z}$: Alice takes a random $k \in \mathbb{Z}\ell\mathbb{Z}$, compute $r = x_{kP} \in \mathbb{Z}/\ell\mathbb{Z}$ and sends

$$r, s = \frac{m + ra}{k}$$

- Verification: Bob computes $v = \frac{m}{s}P + \frac{raP}{s}$ and checks that $x_v = r \mod \ell$.

2 Addition law

- Implement the addition law for elliptic curves in Edwards model:

$$E : x^2 + y^2 = 1 + dx^2y^2, \quad d \neq 0, -1.$$

If $P = (x_1, y_1)$ and $Q = (x_2, y_2)$:

$$P + Q = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

Check that $(0, 1)$ is a neutral element, that $-(x, y) = (-x, y)$ and that $T = (1, 0)$ has order 4 with $2T = (0, -1)$.

- Generalize to twisted Edwards curves:

$$E : ax^2 + y^2 = 1 + dx^2y^2.$$

If $P = (x_1, y_1)$ and $Q = (x_2, y_2)$:

$$P + Q = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}\right).$$

- Montgomery curves:

$$E : By^2 = x^3 + Ax^2 + x$$

One can work using only the x coordinate: we represent a point $\pm P \in E$ by the projective coordinates $(X : Z)$ where $x = X/Z$. No addition when we only have the x-coordinate, but we can do differential additions! Given $\pm P_1 = (X_1 : Z_1)$, $\pm P_2 = (X_2 : Z_2)$ and $\pm(P_1 - P_2) = (X_3 : Z_3)$ then $\pm(P_1 + P_2) = (X_4 : Z_4)$ is given by

$$X_4 = Z_3\left((X_1 - Z_1)(X_2 + Z_2) + (X_1 + Z_1)(X_2 - Z_2)\right)^2$$
$$Z_4 = X_3\left((X_1 - Z_1)(X_2 + Z_2) - (X_1 + Z_1)(X_2 - Z_2)\right)^2$$

Implement the scalar multiplication $\pm P \mapsto \pm nP$ by using a Montgomery ladder: at each step we have $\pm nP, \pm(n + 1)P$ and we compute $\pm 2nP, \pm(2n + 1)P$ or $\pm(2n + 1)P, \pm(2n + 2)P$.

3 Discrete Logarithms

Try to implement the baby step giant step algorithm or the Pollard ρ method for the DLP in $E(\mathbb{F}_q)$.

4 Pairings and Miller's algorithm

Fix a prime ℓ and find an elliptic curve such that $\ell \mid \#E(\mathbb{F}_q)$. Let e be the embedding degree (compute it!)

Let $P \in E[r](\mathbb{F}_q)$ and $Q \in E(\mathbb{F}_{q^e})$. Implement Miller's algorithm algorithm 4.1 to compute $f_{r,P}(Q)$.

We recall that $f_{\lambda,P} \in \mathbb{F}_q(E)$ has divisor $\mathrm{Div}(f_{\lambda,P}) = \lambda[P]-[\lambda P]-(\lambda-1)[0_E]$. If $\lambda, \nu \in \mathbb{N}$, $f_{\lambda+\nu,P} = f_{\lambda,P}f_{\nu,P}\mu_{\lambda P,\nu P}$ where $\mu_{\lambda P,\nu P}$ has divisor $[(\lambda + \nu)P] - [(\lambda)P] - [(\nu)P] + [0_E]$:

$$\mu_{P_1,P_2} = \frac{y - \alpha(x - x_{P_1}) - y_{P_1}}{x + (x_{P_1} + x_{P_1}) - \alpha^2} \tag{1}$$

with $\alpha = \frac{y_{P_1} - y_{P_2}}{x_{P_1} - x_{P_2}}$ when $P_1 \neq P_2$ and $\alpha = \frac{f'(x_{P_1})}{2y_{P_1}}$ when $P_1 = P_2$.

Algorithm 4.1 (Evaluating $f_{r,P}$ on Q).

Input: $r \in \mathbb{N}$, $P = (x_P, y_P) \in E[r](\mathbb{F}_q)$, $Q = (x_Q, y_Q) \in E(\mathbb{F}_{q^d})$.

Output: $f_{r,P}(Q)$ where $\mathrm{Div}\, f_{r,P} = r[P] - r[0_E]$.

1. Compute the binary decomposition: $r := \sum_{i=0}^{I} b_i 2^i$. Let $T = P, f_1 = 1, f_2 = 1$.
2. For i in $[I..0]$ compute
   a) α, the slope of the tangent of E at T.
   b) $f_1 = f_1^2(y_Q - \alpha(x_Q - x_T) - y_T)$, $f_2 = f_2^2(x_Q + 2x_T - \alpha^2)$.
   c) $T = 2T$.
   d) If $b_i = 1$, then compute
      i. α, the slope of the line going through P and T.

ii. $f_1 = f_1^2(y_Q - \alpha(x_Q - x_T) - y_T)$, $f_2 = f_2(x_Q + x_P + x_T - \alpha^2)$.

iii. $T = T + P$.

Return $\frac{f_1}{f_2}$.

- Implement the Weil pairing
$$e_{W,\ell}(P,Q) = \frac{f_{\ell,P}(Q)}{f_{\ell,Q}(P)}$$
for $P, Q \in E[\ell]$;
- Implement the Tate pairing
$$e_{T,\ell}(P,Q) = f_{\ell,P}(Q)^{\frac{q^e-1}{\ell}}$$
for $P \in E[\ell](\mathbb{F}_q)$ and $Q \in E(\mathbb{F}_{q^e})$;
- Compare with the Sage/Pari implementation, check bilinearity.
- Generalize the computation of $f_{r,P}$ to reduce an arbitrary divisor. Optimize the divisor reduction using a double and add algorithm.
- Example: $y^2 = x^3 - 5$ over $\mathbb{F}_p$ with
$$p = 260532200783961536561853044153738822596223089371557168731494664303638395082391$$
check that
$$\#E(\mathbb{F}_p) = 260532200783961536561853044153738822595712665821175760941446444365476223949041$$
is prime and that the embedding degree e is 12. Try some pairings between $P \in E(\mathbb{F}_p)$ and $Q \in E(\mathbb{F}_{p^{12}}[r])$.

5 The group structure of $E(\mathbb{F}_q)$

Let E be an elliptic curve over $\mathbb{F}_q$. Let $N = \#E(\mathbb{F}_q)$ (ask Sage or Pari to get the number of points!). $E(\mathbb{F}_q) = \mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/b\mathbb{Z}$ with $a \mid b$ and we want to compute a and b.

Take P, Q two random points in $E(\mathbb{F}_q)$. Write a naive program to check that they generate $E(\mathbb{F}_q)$.

Here is a faster method: factorize N to compute the order N_1 and N_2 of P and Q. Let $b = N_1 \vee N_2$ and a the order of $e_b(P,Q)$. Prove that $E(\mathbb{F}_q) =< P, Q >$ if and only if $N = ab$. Implement this algorithm.

Hint: using the CRT one can assume that $N = \ell^e$, and we want to find the ℓ-adic valuation of a and b. Also it may be easier to find two generators for each $E[\ell^\infty](\mathbb{F}_q)$ and use the CRT to find two generators for $E(\mathbb{F}_q)$.

Once we have two generators $< P, Q >$ we want to replace them by a linear combination so that P, Q are generators with P of order a and Q of order b. (such generators are said to be in SNF form).

Hint: Likewise work over each $E[\ell^\infty](\mathbb{F}_q)$. This will involve DLP in $E[\ell]$ so don't try with an elliptic curve too big! Why don't we just take random elements until we find generators of the form above?

Example 5.1. Suppose that $E[\ell^\infty](\mathbb{F}_q) = \mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/\ell^2\mathbb{Z}$. The first random point is $P = (0,1)$ and the second is $Q = (1,\alpha)$. Then P and Q are of order ℓ^2 and $e_{\ell^2}(P,Q) \neq 1$ (why?) so P, Q are generators.

$\ell P = \alpha \ell Q$, one can recover α via a DLP in $E[\ell]$, and compute $Q_1 = Q - \alpha P$. Then $Q_1 = (1,0)$ is of ordrer ℓ and Q_1, P is in SNF (Smith Normal Form).

Example 5.2. Let $E : y^2 = x^3 + 723138791x + 549773675$ over $\mathbb{F}_p$ with $p = 777034913$. $\#E(\mathbb{F}_p) = 3 \times 7 \times 17^4 \times 443$. Find the structure of $E[17^\infty](\mathbb{F}_p)$ and generators.

6 DLP in anomalous curves

Exercice provided by Benjamin Smith.

Let

$$p = 11 \cdot 2^{252} + 12188 \cdot 2^{124} + 211005\,.$$

The elliptic curve

$$E/\mathbb{F}_p : y^2 = x^3 - \frac{1536}{539}x + \frac{1024}{539}$$

is anomalous: that is, it has exactly p points.

1. Create E, and check that it has p points (you shouldn't need to use an explicit point counting algorithm).
2. First, implement an augmented group law $\oplus$ on pairs in $E(\mathbb{F}_p) \times \mathbb{F}_p$:

   $$(P, \alpha_P) \oplus (Q, \alpha_Q) := (P + Q, \alpha_P + \alpha_Q + a_0(P, Q))$$

   where $a_0(P, Q)$ is the constant coefficient in the expansion of $(d\mu_{P,Q}/dt)/\mu_{P,Q}$ in terms of $t = x/y$, where $\mathrm{Div}\,\mu_{P,Q} = l_{P,Q}/v_{P,Q}$, where $l_{P,Q}$ is the line through P and Q and $v_{P,Q}$ is the vertical line through $P + Q$ (so $[P] + [Q] - 2[0_E] = [P + Q] - [0_E] + \mathrm{Div}(\mu_{P,Q})$).
3. Now implement a simple double-and-add loop to compute $[m](P, a_P) = (P, a_P) \oplus \cdots \oplus (P, a_P)$ using your augmented group law.
4. Now, generate a random DLP instance: $Q = [m]P$ on $\mathscr{E}$.
5. Compute $[p](P, 0)$ and $[p](Q, 0)$: you should have $[p](P, 0) = (0_{\mathscr{E}}, \alpha)$ and $[p](Q, 0) = (0_{\mathscr{E}}, \beta)$ for some α and β in $\mathbb{F}_p$.
6. Check that $m = \beta/\alpha$.