Courbes elliptiques — 4TMA902U

Responsables : G. Castagnos, D. Robert

Terminal Exam — December 11, 2020

3h

Documents are not allowed

Answer the two parts on separate sheets

G. Castagnos' Part

I Let p be a prime number with $p > 3$ and $p \equiv 3 \pmod 4$. We denote by E the elliptic curve of equation $y^2 = x^3 + x$ over $\mathbf{F}_p$.

(a) Let $x \in \mathbf{F}_p$ and denote $f(x) = x^3 + x$. Show that $f(x)$ is a square if and only if $f(-x)$ is not a square.

(b) Show that $E(\mathbf{F}_p)$ has $p + 1$ points (Hint: one can use the fact that $\mathbf{F}_p$ can be written as $\mathbf{F}_p = \{0, \pm 1, \pm 2, \ldots, \pm(p-1)/2\}$).

(c) Show that there exists $i \in \mathbf{F}_{p^2}$ such that $i^2 = -1$.

In the following, we denote by ϕ the map that sends a point $Q = (x, y)$ of $E(\mathbf{F}_p)$ to $\phi(Q) = (-x, iy)$ and that sends O_E to itself.

(d) Prove that $\phi(Q) \in E(\mathbf{F}_{p^2})$ for all $Q \in E(\mathbf{F}_p)$.

We assume in the following that ϕ is a morphism for the group law of the points of the curve. Moreover, we will assume that there exists a prime factor ℓ of $p+1$ with $\ell > 2$. We will denote $G = \langle P \rangle$ where P is a point of $E(\mathbf{F}_p)$ of order ℓ.

(e) Give an algorithm (in pseudo code or Sage) that takes an integer λ as input, and that outputs (with the previous notations) ℓ of λ bits, the prime p, and the point P.

(f) What is the embedding degree of ℓ in $\mathbf{F}_p$?

(g) Let us denote $P = (x_P, y_P)$ the affine coordinates of P. Show that $y_P \neq 0$. Deduce that P and $\phi(P)$ generate the ℓ–torsion of the curve E.

(h) Show how to define a cryptographic pairing of type I with this curve.

(i) Show how to use this pairing to do a tripartite key exchange in one round between Alice, Bob and Carl.

(j) Suppose that Alice and Bob do a Diffie-Hellman key exchange in the group $G = \langle P \rangle$. Suppose we know the values X and Y exchanged by Alice and Bob. Given and element $Z \in G$ show how to efficiently tell if Z is the secret common quantity established by Alice and Bob.

2 Let ℓ be a large prime number and $(G_1, +)$ and $(G_t, \times)$ be two distinct cyclic groups of the same order ℓ. Let P be a generator of G_1 and $e : G_1 \times G_1 \to G_t$ be a cryptographic bilinear pairing of type I.

Let H be a cryptographic hash function that maps binary strings to elements of G_1. We recall the BLS signature scheme using a type I pairing: The secret signature key is an integer x such that $1 < x < \ell$. The public verification key is $Q = xP \in G_1$. The signature of a binary string m with the secret key x is computed as $\sigma = xH(m) \in G_1$.

(a) What precise problem an attacker must exactly solve in order to compute a valid signature of m for the public key Q without knowing the corresponding secret key x ? Deduce from that the verification algorithm of this signature scheme.

(b) In this question only, we suppose that we sign integers m with $1 < m < \ell$ and that the hash function H consists in computing $H(m) := mP$. Show that an attacker can efficiently build a valid signature of m with the public key Q without knowing the corresponding secret key x.

Let $n > 1$ be an integer. In the following, we suppose that n participants use this BLS signature scheme. For $i = 1, \dots, n$, we denote x_i with $1 < x_i < \ell$, the secret key of participant i and $Q_i = x_i P \in G_1$ its public key. Let $m_1, \dots, m_n$ be messages. For $i = 1, \dots, n$, we denote $\sigma_i \in G_1$ the signature by participant i of the message m_i with the signature scheme.

(c) Show how to combine the signatures $\sigma_1, \dots, \sigma_n$ in a single element σ of G_1 in a way that it is possible, given σ, the messages $m_1, \dots, m_n$ and the public keys $Q_1, \dots, Q_n$ to verify that σ is a combination of signatures by participants 1 to n for messages $m_1, \dots, m_n$. Give this verification procedure.

(d) Let m be a message that participant 1 has never signed. Show that an attacker can pretend to have signed together with participant 1 this plaintext m: that is to say, show that an attacker, without knowing neither x_1 nor the signature of participant 1 for m, can produce a public key Q_a and $\sigma \in G_1$ such that the input σ, m, m, Q_1, Q_a is accepted by the verification procedure given in the previous question.

Propose a countermeasure to this attack.

D. Robert's Part

3

(a) Give the binary decomposition of $\ell = 37$.

(b) Let E be an elliptic curve, $P \in E$. Explain which precomputation we would make and what intermediate points we would get when computing $\ell.P$ for $\ell = 37$ via the left to right method, a window of length 2, a window of length 3, and a sliding window of length 2.

(c) Recall the definition and the explicit form of the function $\mu_{P,Q}$ for $P, Q \in E$.

(d) Recall the definition of the function $f_{\ell,P}$.

(e) Show that

$$f_{\ell_1+\ell_2,P} = f_{\ell_1,P} f_{\ell_2,P} \mu_{\ell_1 P,\ell_2 P} \tag{1}$$

(f) Explain what is Miller's algorithm to compute $f_{\ell,P}$. Then explain how we would compute $f_{37,P}$ with Miller's algorithm.

(g) Explain how to adapt Miller's algorithm to use a window of size 2, of size 3 and a sliding window of size 2 for $\ell = 37$. Which precomputation do we need to make in each case?

Remark: For the last two questions, just explain for which values we would use (1), there is no need to give the explicit values of the functions $\mu_{\ell_1 P,\ell_2 P}$ each time.

4 This exercice is in two independent parts. (Part B reuse the notations for Part A but does not require having done Part A).

Part A

Let $\mathbf{F}_q$ be a finite field, q odd, and $E : y^2 = x^3 + ax + b$ an elliptic curve over $\mathbf{F}_q$.

(a) Show that $\mathbf{F}_q^*/\mathbf{F}_q^{*,2} \simeq \mathbf{Z}/2\mathbf{Z}$.

(b) Deduce that there is always a $u \in \mathbf{F}_q^*$ such that u is not a square in $\mathbf{F}_q$. If we take $u \in \mathbf{F}_q^*$ at random, what is the probability that it is a square?

(c) Let $u \in \mathbf{F}_q^*$, give a short Weierstrass equation (via a change of variable) of $E_u : uy^2 = x^3+ax+b$.

(d) Recall what are the isomorphisms of short Weierstrass equations. Deduce that the isomorphism class of E_u over $\mathbf{F}_q$ only depends on the value of u in $\mathbf{F}_q^*/\mathbf{F}_q^{*,2}$. In other words: if $u \in \mathbf{F}_q^{*,2}$, $E_u \simeq E$ over $\mathbf{F}_q$, if $u \notin \mathbf{F}_q^{*,2}$, $E_u \not\simeq E$ over $\mathbf{F}_q$ and if $u, u' \notin \mathbf{F}_q^{*,2}$, $E_u \simeq E_{u'}$ over $\mathbf{F}_q$.

(e) Show that E_u is always isomorphic to E over $\mathbf{F}_{q^2}$.

(f) If E' is an elliptic curve isomorphic to E_u, $u \notin \mathbf{F}_q^{*,2}$, we say that E' is a quadratic twist of E. Explain why a quadratic twist of E always exist, is not isomorphic to E over $\mathbf{F}_q$ but is isomorphic to E over $\mathbf{F}_{q^2}$.

(g) Fix $u \notin \mathbf{F}_q^{*,2}$. Show that if $z \in \mathbf{F}_q^*$, either z is a square, or (exclusive) uz is a square.

(h) Deduce that if E′ is a quadratic twist of E, $\#E + \#E' = 2q + 2$.

(i) Recall the definition of the characteristic polynomial of the Frobenius χ_π and how we can compute $\#E(\mathbf{F}_q)$ from χ_π.

(j) Show that if E′ is a quadratic twist of E and π' the Frobenius of E′, then $\chi_{\pi'}(X) = \chi_{\pi'}(-X)$. Deduce that $\pi' = -\pi$.

(k) Show that if $\chi_\pi = X^2 - tX + q$, then $\chi_{\pi^2} = X^2 - (t^2 - 2q) + q^2$. Explain how to compute $\#E(\mathbf{F}_{q^2})$ from $\#E(\mathbf{F}_q)$.

(l) Check that $\#E(\mathbf{F}_{q^2}) = \#E(\mathbf{F}_q)\#E'(\mathbf{F}_q)$ (E′ a quadratic twist). Deduce that if $2 \nmid \#E(\mathbf{F}_q)$, $E(\mathbf{F}_{q^2}) \simeq E(\mathbf{F}_q) \oplus E'(\mathbf{F}_q)$.

Part B

Assume that E is such that $\ell \mid \#E(\mathbf{F}_q)$, $\ell^2 \nmid \#E(\mathbf{F}_q)$, and $k > 1$ where k is the embedding degree.

(m) Recall the definition of the embedding degree, of the Weil pairing $e_{W,\ell}$, and of the (reduced) Tate pairing $e_{T,\ell}$.

(n) Let π be the Frobenius morphism. Define $\mathbf{G}_2 = \mathrm{Ker}(\pi - [q])$ and $\mathbf{G}_1 = \mathrm{Ker}(\pi - [1])$ in $E[r]$. In which extension does the points of $\mathbf{G}_1$ live? Meaning what is the smallest extension $\mathbf{F}_{q^d}$ containing all the points $\mathbf{G}_1(\overline{\mathbf{F}}_q)$? Same question for $\mathbf{G}_2$. Deduce on which extension all the points of $E[\ell]$ live.

(o) Assume that $k = 2k'$ is even. Show that $q^{k'} \equiv -1 \pmod{\ell}$.

(p) Let $u \notin \mathbf{F}_q^{*,2}$, and define $E_u : uy^2 = x^3 + ax + b$. Let $v \in \mathbf{F}_{q^2}$ such that $u = v^2$. Using v define an isomorphism $\xi : E \to E_u$ over $\mathbf{F}_{q^2}$ and show that $\pi(\xi(P)) = \xi(-\pi(P))$.

(q) Show that the points of $\xi(\mathbf{G}_1)$ live in $E(\mathbf{F}_{q^2})$.

(r) Assume that $k = 2k'$ and k' is odd. Show that the points of $\xi(\mathbf{G}_2)$ live in $E(\mathbf{F}_{q^{k'}})$.

(s) Explain how to use ξ to speed up the computation of the Tate pairing on $\mathbf{G}_2 \times \mathbf{G}_1$.