Advanced Cryptology - Final Exam - (3 h)

Documents allowed. No computer, cellphone off.

Exercise 1.

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

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) 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.

Exercise 2.

Let T be the set of monomials of $K[X_1, \dots, X_n]$, endowed with a monomial order $\preccurlyeq$. We consider an ideal I of $K[X_1, \dots, X_n]$; let G be a Gröbner basis of I. We define the *staircase* of I to be the set

$$O(I) = \{m \in T : m \notin \mathrm{lt}(I)\} = \{m \in T : \ m \neq \mathrm{lm}(f) \ \forall f \in I\}.$$

A *corner* of the staircase is a monomial $m \in T \backslash O(I)$ such that

$$\forall m' \in T \backslash O(I), \ m' | m \Rightarrow m' = m.$$

1. Show that a monomial m belongs to $O(I)$ if and only if $\mathrm{lm}(g) \nmid m$ for all $g \in G$.
2. Let $f \in K[X_1, \dots, X_n]$ be a polynomial. Show that $\overline{f}^G$ belongs to the vector space $Span_K(O(I))$ generated by the monomials of the staircase of I.
3. Prove that the corners of $O(I)$ are exactly the leading monomials of the elements of a minimal Gröbner basis of I.
4. Let I be an ideal of $K[x, y, z]$ whose staircase is $O(I) = \{1, x, y, y^2, xy, z\}$. Determine its corners.
5. Let $I = \langle x^2y - 1, xy^2 - x\rangle \in \mathbb{R}[x, y]$ endowed with the lexicographical order (with $x > y$). Compute a Gröbner basis of I and deduce its staircase.

Barkee's cryptosystem. In a pseudonymous article, Barkee and his co-authors proposed the following public-key encryption outline (with the goal of showing that it *cannot* be secure).

- Key generation: Alice generates an ideal $I \subset K[X_1, \dots, X_n]$ (with K a finite field), a Gröbner basis $G = \{g_1, \dots, g_s\}$ of I and a set $F = \{f_1, \dots, f_t\}$ such that $\langle F\rangle = I$. The details are not specified, but the idea is to start from G; computing a Gröbner basis of I starting from F is supposed to be computationally hard. The public key consists of F and $O(I)$ (or just a subset of $O(I)$), the private key is G.
- Encryption: plaintexts are encoded as elements of $Span_K(O(I))$. To encrypt $M = \sum_{m \in O(I)} c_m m$, Bob selects random degree r polynomials $p_1, \dots, p_t$ and outputs $C = M + \sum_{i=1}^t p_i f_i$.
- Decryption: Alice decrypts a ciphertext C by computing its normal form $\overline{C}^G$ with respect to the Gröbner basis G.

4. Prove that this system is correct, i.e. decryption works.
5. A chosen-ciphertext attack:
   (a) Let g be a monic element of a minimal reduced Gröbner basis of I. Show that for any polynomials $p_1, \dots, p_t$, the following equality holds:
   $$\overline{\mathrm{lm}(g) + \sum_i p_i f_i}^G = \mathrm{lm}(g) - g.$$
   (b) Use this result to describe a chosen-ciphertext attack on this cryptosystem, in the case where the whole set $O(I)$ is public. Generalize it to an adaptative chosen-ciphertext attack in the case where only a subset of $O(I)$ is public.

Exercise 3.

Let $\mathcal{H}$ be the genus 5 hyperelliptic curve defined over $\mathbb{F}_2$, of equation

$$y^2 + (x^5 + x^2 + 1)y = x^{11} + x^{10} + x^3 + x^2.$$

Its (unique) point at infinity is noted O. The Jacobian of $\mathcal{H}$ has 86 $\mathbb{F}_2$-rational elements. We consider the divisor classes (given in Mumford representation)

$$D_0 = (x^4 + x^3, x^3 + x^2), \qquad D_1 = (x^5 + 1, x^3 + x).$$

The order of D_0 in $\mathrm{Jac}_{\mathcal{H}}$ is 86; let s be the discrete logarithm of D_1 in base D_0, i.e. the unique integer (modulo 86) such that $D_1 = sD_0$.

1. Give all the $\mathbb{F}_2$-rational points of $\mathcal{H}$. For each $P \in \mathcal{H}(\mathbb{F}_2)$, write down the Mumford representation of the divisor $(P) - (O)$ and of its opposite in $\mathrm{Jac}_{\mathcal{H}}$.

In what follows, we will consider the two divisor classes $u_0 = (x, 0)$ and $u_1 = (x + 1, 0) \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_2)$, given in Mumford representation, and the factor base $\mathcal{F} = \{u_0, u_1\}$.

2. Give the factorization of $x^4 + x^3$ in $\mathbb{F}_2[x]$. Deduce a decomposition of D_0 over $\mathcal{F}$, i.e. a relation $D_0 = \lambda u_0 + \mu u_1$ with $\lambda, \mu \in \mathbb{Z}$.
3. Compute similar decompositions of $2D_0 = (x^4, x^3 + 1)$ and of $D_0 + D_1 = (x^5 + x^4 + x^3 + x^2, x^4 + x^3 + 1)$.
4. Combine the above decompositions to find a non-trivial relation of the form $aD_0 + bD_1 = 0$.
5. Is this relation enough to deduce the value of s modulo 86? modulo a factor of 86?
6. A simple computation yields $43D_1 \neq (1, 0)$. Deduce the value of s modulo 2, and finally the value of s modulo 86.

Exercise 4.

Let E be the elliptic curve defined over $\mathbb{F}_2$ with Weierstrass equation

$$y^2 + xy = x^3 + x^2 + 1.$$

1. Give the characteristic polynomial of the Frobenius endomorphism $\Phi_2 : (x, y) \mapsto (x^2, y^2)$ of E.
2. Is this curve supersingular?
3. Compute the number of $\mathbb{F}_4$-rational points of E.
4. Is there any extension of $\mathbb{F}_2$ on which the number of rational points of E is prime? What are the pros and cons of the use of this curve for cryptographic applications?

5. Let $\mu \in \mathbb{C}$ be a complex number such that $\mu^2 - \mu + 2 = 0$, and let n be an arbitrary integer. We consider the sequence (a_k) with integer values, and the sequence (ϵ_k) with values in $\{0, 1\}$, defined by the relations

$$a_{-1} = 0, \quad a_0 = n, \quad a_{k+1} = \lfloor \frac{a_k}{2} \rfloor - \lfloor \frac{a_{k-1}}{2} \rfloor,$$

$$\epsilon_k = a_k - 2\lfloor \frac{a_k}{2} \rfloor = a_k \bmod 2.$$

Prove by induction that for all $k \in \mathbb{N}$,

$$n = \sum_{i=0}^{k-1} \epsilon_i \mu^i + a_k \mu^k - \lfloor \frac{a_{k-1}}{2} \rfloor \mu^{k+1}.$$

6. Compute the sequence (ϵ_k) for $n = 7$.

7. We admit that for all $n \in \mathbb{N}$, the sequences (a_k) and (ϵ_k) only have a finite number of non-zero values. Thus every integer has an expansion in base μ , of the form $n = \sum_{i=0}^{r} \epsilon_i \mu^i$ with $\epsilon_i \in \{0, 1\}$. How this expansion can be used to compute $[n]P$ where $P \in E(\mathbb{F}_{2^d})$?

8. Write down the integer 7 in base 2 and in base μ. What can be remarked about the length of these expressions? Conclude about the applications to cryptography.