Advanced Crypto – Exercises

Analysis of the KZG polynomial commitment scheme

We recall that in the KZG scheme, the participants have access to public parameters $P, sP, \dots, s^d P, Q, sQ$ where s is a secret integer, P and Q are points of large prime order p on a pairing friendly elliptic curve E defined over a finite field, such that the pairing $e(P, Q) \neq 1$, and d is an integer such that d/p is negligible.

The commitment of a polynomial $f = \sum_{k=0}^{d} a_k X^k \in \mathbb{F}_p[X]_{\leq d}$ is the point $\mathrm{Commit}(f) = f(s)P = \sum_{k=0}^{d} a_k(s^k P)$.

1. **Computational binding.**
   Assume that a participant is able to find two polynomials $f, g \in \mathbb{F}_p[X]_{\leq d}$ such that $\mathrm{Commit}(f) = \mathrm{Commit}(g)$. Show that he is then able to compute s.
   Hint: there exists an efficient probabilistic algorithm to find the roots of a univariate polynomial over a finite field

2. **Statistical hiding.**
   Explain why the KZG commitment is not perfectly Zero-Knowledge. Nethertheless is it possible to recover f from a commitment c?

We recall the evaluation procedure. A participant knowing f can produce a proof Π that $f(y) = z$ (for some $y, z \in \mathbb{F}_p$) by computing the polynomial $h = \frac{f(X)-z}{X-y} = \sum_{k=0}^{d-1} b_k X^k$ and outputing $\Pi = h(s)P = \sum_{k=0}^{d-1} b_k(s^k P)$.

To verify the proof Π that $f(y) = z$ knowing only $C = \mathrm{Commit}(f)$, one checks if $e(\Pi, sQ - yQ) = e(C - zP, Q)$.

3. **Evaluation binding.**
   The commitment scheme is *evaluation binding* if it is not possible to produce a tuple (C, Π, y, z) passing the verify procedure without knowing a polynomial f such that $C = \mathrm{Commit}(f)$ and $f(y) = z$. This can be modelled by a knowledge extraction.
   More simply, we consider the commitment scheme to be evaluation binding if an adversary cannot produce two tuples (C, π_0, y, z_0) and (C, π_1, y, z_1) that pass the verify procedure with $z_0 \neq z_1$.

   (a) Show that if (C, π_0, y, z_0) and (C, π_1, y, z_1) pass the verify procedure (with $z_0 \neq z_1$), then
   $$\frac{1}{z_1 - z_0}(\Pi_0 - \Pi_1) = \frac{1}{s-y}P.$$

   (b) Assume the computational hardness of the *d-strong Diffie-Hellman problem* :
   $$\text{given } P, sP, \dots, s^d P, \text{ ouput a couple } (c, \tfrac{1}{s-c}P).$$
   Show that the KZG commitment scheme is then evalutation binding.

4. **Evaluation hiding.**
   The commitment scheme is *evaluation hiding* if an evaluation proof π reveals "nothing more" than the fact that $f(y) = z$. We are going to show that if there exists an algorithm $\mathcal{A}$ that:

   - takes as input setup points $(P, sP, \dots, s^d P, Q, sQ)$, a commitment C of a polynomial $f \in \mathbb{F}_p[X]_{\leq d}$ as well as t valid evaluation proofs $((\Pi_i, y_i, z_i))_{1 \leq i \leq t}$ for the commitment C where $t \leq d$
   - outputs in polynomial time f with non negligible probability

   then it is possible to compute discrete logarithm in E.

   (a) What is the rationale behind the condition $t \leq d$?

Assume Bob has access to such an algorithm $\mathcal{A}$, and wants to compute the discrete log of a point $P' = aP$ in base P. He chooses an integer s and starts by computing $(P, sP, \ldots, s^d P, Q, sQ)$. He then computes the polynomial $L = \frac{(-1)^t}{t!} \prod_{i=1}^{t} (X - i)$ and sets $f = aL + X$.

(b) Give the value of $f(0)$ and $f(i)$ for $1 \leq i \leq t$.

(c) Although Bob does not know a (and thus f), explain how he can compute $C = f(s)P$ as well as $\Pi_i = \frac{f(s)-i}{s-i} P$ for all $1 \leq i \leq t$.

(d) Bob feeds $\mathcal{A}$ with the inputs $(P, sP, \ldots, s^d P, Q, sQ)$, C and $((\Pi_i, i, i))_{1 \leq i \leq t}$.
Show that all the evaluation proofs pass the verification test. How can Bob recover the dicrete log a (with non-negligible probability) from the output of $\mathcal{A}$?

5. **Homomorphic property.**
Let (Π_1, y, z_1) be a valid evaluation proof for the KZG commitment C_1, and (Π_2, y, z_2) a valid evaluation proof for the commitment C_2, for the same setup points $(P, sP, \ldots, s^d P, Q, sQ)$.
Show that $(\Pi_1 + \Pi_2, y, z_1 + z_2)$ is a valid evalution proof for $C_1 + C_2$.

6. **Zero-knowledge KZG commitments**
For the zero-knowledge version of the KZG scheme, the setup phase is modified: two points P and P' are chosen in $E(\mathbb{F}_q)[p]$, and the common reference points are now $(P, sP, \ldots, s^d P, P', sP', \ldots, s^d P', Q, sQ)$. The integer s remains secret, and P and P' are chosen independently so that no user knows the discrete log of P' in base P.
In order to commit a polynomial $f \in \mathbb{F}_p[X]_{\leq d}$, a user now chooses a random polynomial $f' \in \mathbb{F}_p[X]_{\leq d}$ and compute $C = f(s)P + f'(s)P'$ using the reference points.

(a) Show that this commitment is zero-knowledge (C gives absolutely no information on f).

(b) Show that this commitment is computationally binding, assuming the hardness of a DL-based problem that has to be explicited.

(c) Explain how to modify the evaluation procedures (generation and verification of a proof).