ZKP IAP: Session 5 Homework

Brian Justin Stout*

September 28, 2023

Problem 1. *How can use the secret value τ to make a fake KZG opening proof if you had it?*

Suppose verifer sends y and I desire to send $w \neq z = f(y)$ with a proof $\pi = g^n$ that satisfies the pairing.

The verifier will check the pairing formula, where c_f is the commitment to f:

$$e(\frac{c_f}{g^w}, g) = e(\pi, \frac{g^\tau}{g^y})$$

$$= e(f^{f(\tau)-w}, g) = e(g^n, g^{\tau-y})$$
$$= e(g,g)^{f(\tau)-w} = e(g,g)^{n(\tau-y)}$$

Which will hold if we compute π using $n = \dfrac{f(\tau)-w}{\tau-y}$, and is computable if we know τ.

Problem 2. *Construct a vector commitment scheme from the ZKG polynomial commitment scheme.*

Suppose our message space was $\mathcal{M} = \mathbb{F}^n = \{(m_1, ..., m_n) | m_i \in \mathbb{F}\}$. Let $m \in \mathcal{M}$ be a message. Construct the ordered pairs

$$(1, m_1), ..., (n, m_n)$$

and let f_m be the degree $n-1$ polynomial over $\mathbb{F}$ defined by Lagrange interpolation. Finally, define the commitment of m to be the ZKG commitment of f_m, which we denote by c_m.

The commitment scheme is defined as follows:

- $Setup(1^\lambda)$ is the same as the ZKG set up, assuming $d > n$. Outputs $SRS = (ck, vk)$
- $Commit(ck, m)$ produces c_m the ZKG commitment to f_m.
- $Open(SRS, c_m, i, m_i)$ produces a ZKG proof that $f_m(i) = m_i$.

*email: bjstout@proton.me

Problem 3. *Can you extend ZKG polynomial commitment scheme to produce a multiproof π that convinces us of $p(x_i) = y_i$ for a list of points and evaluations (x_i, y_i)?*

Suppose we had a commitment to a polynomial p and had several challenges (x_i, y_i) for $i = 1, ..., r$. Interpolate $I(x)$ using Lagrange interpolation. Then $p(x) - I(x)$ has roots at $x_1, ..., x_r$ and therefore $\Pi_i(x - x_i)$ divides this polynomial. Let q be the quotient polynomial. Set the opening proof $\pi = [q(\tau)]_1$.

We claim this opening proof will validate with any (x_i, y_i). The pairing check is:

$$e(\frac{c_p}{g^{y_i}}, g) = e(\pi, \frac{g^\tau}{g^{x_i}})$$
$$= e(g, g)^{p(\tau)-y_i} = e(g, g)^{q(\tau)(\tau-x_i)}$$

which holds since the interpolated polynomial $I(x_i) = y_i$.