Homework 10

Groth16 Part 1

Use a QAP from an earlier homework as a starting point.

The trusted setup should generate the following values:

$$\tau, \alpha, \beta$$

which are the “toxic waste” (read this https://www.coindesk.com/layer2/2022/01/26/what-is-zcash-the-privacy-coin-explained/).

Notation

Bold letters are vectors

$$\langle \mathbf{a}, \mathbf{b} \rangle$$

Is an inner product between vectors **a** and **b**.

$$[A]_1$$

Is a G1 point

$$[B]_2$$

Is a G2 point

$$I_{12}$$

Is the identity in G12

Carry out the following computations in Python:

Trusted Setup

Generate the powers of tau for A and B:

$$[\tau^d G_1, \tau^{d-1} G_1, ..., \tau G_1, G_1]$$

$$[\tau^d G_2, \tau^{d-1} G_2, ..., \tau G_2, G_2]$$

$$[\dots, \tau^2 t(\tau) G_1, \tau t(\tau) G_1, t(\tau) G_1]$$

$$\Psi_i = (w_i(\tau) + \alpha v_i(\tau) + \beta u_i(\tau)) G_1 \quad \text{for i = 1 to m}$$

The trusted setup publishes

$$\begin{aligned} [\alpha]_1 &= \alpha G_1 \\ [\beta]_2 &= \beta G2 \\ \boldsymbol{\Psi} &= (w_i(\tau) + \alpha v_i(\tau) + \beta u_i(\tau)) G_1 |_{i=1}^{m} \end{aligned}$$

Prover

The prover computes their witness vector **a** and computes:

$$[A]_1 = [\alpha]_1 + \sum_{i=1}^{m} a_i u_i(\tau)$$

$$[B]_2 = [\beta]_2 + \sum_{i=1}^{m} a_i v_i(\tau)$$

$$[C]_1 = \sum_{i=0}^{m} a_i \mathbf{\Psi}_i + \langle \mathbf{h}, \eta \rangle$$

Verifier

The verifier computes:

$$\mathrm{I}_{12} \overset{?}{=} \mathrm{neg}([A]_1) \cdot [B]_2 + [\alpha]_1 \cdot [\beta]_2 + [C]_1 G_1$$

If you get very stuck, feel free to refer to past implementations by students (which have been published on GitHub).