Homework 8: Encrypted QAP

Given an R1CS, you should transform it into a QAP (you can use the code from the RareSkills ZK Book for this).

This will produce polynomials U, V, W, and HT (see the notation in the book).

Do an encrypted evaluation of each of these polynomials, this will result in

$$
\begin{gathered}
eval(U) = [A]_1 \\
eval(V) = [B]_2, \\
eval(W) = [C']_1, \\
eval(HT) = [HT]_1
\end{gathered}
$$

Create

$$[C] = [C']_1 + [HT]_1$$

Then verify that

$$\text{pairing}([A]_1, [B]_2) - \text{pairing}([C]_1, [G]_2) = 0$$

Do the verification on chain.

Your code should be able to start with an arbitrary R1CS and compute the three elliptic curve points

$$[A]_1, [B]_2, [C]_1$$

for which the verifier will check if the pairing is correct.