Modern Zero Knowledge Cryptography - MIT IAP, 2023.1

# Homework 5: Commitment Schemes

18 January 2023

*Lecturer: Ying Tong*

1. The Setup phase of the KZG polynomial commitment scheme involves computing commitments to powers of a secret evaluation point $\tau$. This is called the "trusted setup" and is often generated in a multi-party computation known as the "Powers of Tau" ceremony. One day, you find the value of $\tau$ on a slip of paper. How can you use it to make a fake KZG opening proof?

2. Construct a **vector commitment scheme** from the KZG polynomial commitment scheme. (Hint: For a vector $m = (m_1, \ldots, m_q)$, is there an "interpolation polynomial" $I(X)$ such that $I(i) = m[i]$?)

   **Fun fact:** *The Verkle tree [1] is a Merkle tree that uses a **vector commitment** instead of a hash function. Using the KZG vector commitment scheme, can you see why a Verkle tree is more efficient?*

3. The KZG polynomial commitment scheme makes an opening proof $\pi$ for the relation $p(x) = y$. Can you extend the scheme to produce a multiproof $\pi$, that convinces us of $p(x_i) = y_i$ for a list of points and evaluations $(x_i, y_i)$? (Hint: assume that you have an interpolation polynomial $I(X)$ such that $I(x_i) = y_i$.

# References


[1] J. Kuszmaul. Verkle trees. `https://math.mit.edu/research/highschool/primes/materials/2018/Kuszmaul.pdf`, 2019.