EE 465: Cryptocurrency and Blockchain Technologies (Autumn 2018)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Assignment 6: 20 points — Date: October 22, 2018

1. [5 points] Let $C(a, x) = xG + aH$ be a Pedersen commitment to an amount a with blinding factor x. Show that this commitment scheme is **not binding** if the discrete log of H with respect to G is known.

2. [5 points] Show the steps involved in calculating a LSAG signature over four public keys P_0, P_1, P_2, P_3 where the signer knows the private key corresponding to P_3.

3. [5 points] Suppose we replace calculation of c_j in the LSAG signature scheme with $c_j = H_s(m, L_{j-1}, I)$ where I is the key image. Show that the scheme loses the linkability property.

4. [5 points] Suppose we want to construct a range proof for a Pedersen committed amount using its base-4 representation, i.e. $a = \sum_{i=0}^{15} a_i 4^i$ where each $a_i \in \{0, 1, 2, 3\}$. We want to show that $a \in \{0, 1, 2, \ldots, 4^{16} - 1\}$ using $C(a, x)$. Show how this can be done using Pedersen commitments $C_i = C(a_i 4^i, x_i)$.