Operating System: Nachos Phase 1 Design Document

Instructed by *Xu Wei*

Due on March 11, 2014

Yin HeZheng Yao Class 2011012343

Algorithm 1 A'(n, e, y)

1: Run A on input (n, e, y)
2: A outputs in time T_A a commitment c and openings $(r_0, 0)$ and $(r_1, 1)$
3: **return** $x = r_0 r_1^{-1} \mod n$

Algorithm 2 A'(g, h)

1: Run A on input (q, g, h)
2: A outputs in time T_A a commitment c and openings $(r_0, 0)$ and $(r_1, 1)$
3: **return** $x = r_0 - r_1 \mod q$

Algorithm 3 M_{V^*}

1: **for** $i = 0$ to ℓ **do**
2: M send M_{V^*} a_i, then M_{V^*} send a_i to V^*
3: M_{V^*} chooses c_i randomly from $\{0, 1\}$
4: Receive b_i from V^*. If $b_i \neq c_i$, rewind and return to line 2 (still in round i). If $b_i = c_i$, then M_{V^*} send b_i to M, M sends M_{V^*} z_i.
5: Write (a_i, b_i, z_i) on the transcript.
6: **end for**