Algorithm 1 KeyGen with NIZKPoP Prover

$v_k \xleftarrow{\$} \chi_q \quad \forall k \in \{1, \dots, M\}$

$seed_{ij} \xleftarrow{\$} \{0,1\}^{256} \quad \forall (i,j) \in \{1, \dots, N-1\} \times \{1, \dots, \tau\}$

$v_{ij} := \mathrm{SampleUniform}(seed_{ij}) \in \mathbb{Z}_q^M \quad \forall (i,j) \in \{1, \dots, N-1\} \times \{1, \dots, \tau\}$ ▷ SHAKE

$v_{Njk} := v_k - \sum_{i=1}^{N-1} v_{ijk} \quad \forall (j,k) \in \{1, \dots, \tau\} \times \{1, \dots, M\}$

$h_{ij} := H(seed_{ij}) \quad \forall (i,j) \in \{1, \dots, N-1\} \times \{1, \dots, \tau\}$ ▷ H is instantiated with SHAKE

$h_k := H(v_k) \quad \forall k \in \{1, \dots, M\}$

$h := H(\{h_{ij}, h_k\})$

with h as input, sample $M - \sigma$ pairwise distinct indices b_k from $\{1, \dots, M\}$ ▷ SHAKE

compose matrices S_{ij}, E_{ij} (each $n \times \bar{n}$) from v_{ijk} where $k \notin \{b_k\}$

compose $n \times \bar{n}$ matrices S, E from v_k where $k \notin \{b_k\}$ ▷ one has $S = \sum_{i=1}^{N} S_{ij} \forall j$ and $E = \sum_{i=1}^{N} E_{ij} \forall j$

generate $n \times n$ matrix A

$B := AS + E$

$B_{ij} := AS_{ij} + E_{ij} \quad \forall (i,j) \in \{1, \dots, N\} \times \{1, \dots, \tau\}$

$h_{B_{ij}} := H(B_{ij}) \quad \forall (i,j) \in \{1, \dots, N\} \times \{1, \dots, \tau\}$

$h_B := H(\{h_{B_{ij}}\})$

with $h, v_{ijk}, h_B, B, A \forall (i,j,k) \in \{1, \dots, N\} \times \{1, \dots, \tau\} \times \{b_k\}$ as input, sample hidden party $r_j \in \{1, \dots, N\}$ for each $j \in \{1, \dots, \tau\}$

return $pk = (A, B), sk = S$ and the proof:

- all b_k
- all r_i
- h
- h_B
- $h_k \forall k \in \{1, \dots, M\} \setminus \{b_k\}$
- $h_{r_j j} \forall j \in \{1, \dots, \tau\} \wedge r_j \neq N$
- $v_{ijk} \forall (i,j,k) \in \{1, \dots, N\} \times \{1, \dots, \tau\} \times \{b_k\}$
- $B_{r_j j} \forall j \in \{1, \dots, \tau\}$
- $S_{Nj}, E_{Nj} \forall j \in \{l : r_l \neq N\}$
- $seed_{ij} \forall (i,j) \in (\{1, \dots, N-1\} \times \{1, \dots, \tau\}) \setminus \{(r_l, l) : 1 \leq l \leq \tau\}$

Algorithm 2 NIZKPoP Verifier

check if $|\sum_{i=1}^{N} v_{ij0}| \leq s$ for all $j \in \{1, \dots, \tau\}$

check if $\sum_{i=1}^{N} v_{i0k} = \sum_{i=1}^{N} v_{ijk}$ for all $(j,k) \in \{2, \dots, \tau\} \times \{b_k\}$

compute S_{ij}, E_{ij} for all $i \notin \{r_j\}$

compute B_{ij} for all $i \notin \{r_j\}$

check if $B = \sum_{i=1}^{N} B_{ij}$ for all $j \in \{1, \dots, \tau\}$

check if $h_B = H(\{H(B_{ij})\})$

compute $h_{ij} := H(seed_{ij})$ for all $(i,j) \in (\{1, \dots, N-1\} \times \{1, \dots, \tau\}) \setminus \{(r_l, l) : 1 \leq l \leq \tau\}$

compute $h_k := H(\sum_{i=1}^{N} v_{i0k})$ for all $k \in \{b_k\}$

check if $h = H(\{h_{ij}, h_k\})$

sample b_k^* from h and check if equal to b_k

sample r_j^* from $h, v_{ijk}, h_B, B, A \forall (i,j,k) \in \{1, \dots, N\} \times \{1, \dots, \tau\} \times \{b_k\}$ and check if equal to r_j