Algorithm 1 Groth16 zk-SNARK Approach

Require: Bilinear groups $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ of prime order p with pairing e
Require: QAP $\{A_i, B_i, C_i\}_{i=0}^{m}$, $t(X)$ with l public inputs

function SETUP
  $\alpha, \beta, \gamma, \delta, x \leftarrow \mathbb{F}_p^*$
  $\text{pk} \leftarrow \begin{pmatrix} [\alpha]_1, [\beta]_1, [\delta]_1, [\delta]_2, \\ \{[A_i(x)]_1, [B_i(x)]_1, [C_i(x)]_1\}_{i=0}^{m}, \\ \{[\frac{\beta A_i(x)+\alpha B_i(x)+C_i(x)}{\gamma}]_1\}_{i=0}^{l}, \\ \{[\frac{\beta A_i(x)+\alpha B_i(x)+C_i(x)}{\delta}]_1\}_{i=l+1}^{m} \end{pmatrix}$
  $\text{vk} \leftarrow \begin{pmatrix} [\alpha]_1, [\beta]_2, [\gamma]_2, [\delta]_2, \\ \{[\frac{\beta A_i(x)+\alpha B_i(x)+C_i(x)}{\gamma}]_1\}_{i=0}^{l} \end{pmatrix}$
  return (pk, vk)

function PROVE(pk, $\{a_i\}_{i=1}^{l}$, $\{a_i\}_{i=l+1}^{m}$)
  $a_0 \leftarrow 1$
  Compute $h(X)$ s.t. $(\sum a_i A_i)(\sum a_i B_i) - \sum a_i C_i \equiv h \cdot t$
  $r, s \leftarrow \mathbb{F}_p$
  $A \leftarrow [\alpha + \sum_{i=0}^{m} a_i A_i(x) + r\delta]_1$
  $B \leftarrow [\beta + \sum_{i=0}^{m} a_i B_i(x) + s\delta]_2$
  $C \leftarrow [\frac{\sum_{i=l+1}^{m} a_i(\beta A_i(x)+\alpha B_i(x)+C_i(x))+h(x)t(x)}{\delta} + sA + rB' - rs\delta]_1$ ▷ $B' = [\beta + \sum_{i=0}^{m} a_i B_i(x)]_1$
  return $\pi = (A, B, C)$

function VERIFY(vk, $\{a_i\}_{i=1}^{l}$, $\pi = (A, B, C)$)
  $a_0 \leftarrow 1$
  $V \leftarrow \sum_{i=0}^{l} a_i \left[\frac{\beta A_i(x)+\alpha B_i(x)+C_i(x)}{\gamma}\right]_1$
  if $e(A, B) \neq e([\alpha]_1, [\beta]_2) \cdot e(V, [\gamma]_2) \cdot e(C, [\delta]_2)$ **then**
    return 0 ▷ Reject
  return 1 ▷ Accept