Algorithm 1 *hybrid key − switching*

Input: $P = \{P_{\mathcal{A}_i}\}_{0 \le i < dnum'}$

$\mathbf{evk_0} = \{\mathbf{evk_{0}}_i\}_{0 \le i < dnum'}$

$\mathbf{evk_1} = \{\mathbf{evk_{1}}_i\}_{0 \le i < dnum'}$

Output: $res0_{\mathcal{A}}, res1_{\mathcal{A}}$

1: **for** $i \leftarrow 0 : dnum' - 1$ **do**
2: $P_{\mathcal{A}_i} = intt(P_{\mathcal{A}_i})$
3: $P_{\mathcal{C}/\mathcal{A}_i} = Bconv(P_{\mathcal{A}_i}, \mathcal{C}/\mathcal{A}_i)$
4: $P_{\mathcal{C}} = ntt(P_{\mathcal{C}/\mathcal{A}_i}) \cup P_{\mathcal{A}_i}$
5: $res0_{\mathcal{C}} = res0_{\mathcal{C}} + PMult(\mathbf{evk_{0}}_i, P_{\mathcal{C}})$
6: $res1_{\mathcal{C}} = res1_{\mathcal{C}} + PMult(\mathbf{evk_{1}}_i, P_{\mathcal{C}})$
7: **for** $i \leftarrow 0 : 1$ **do**
8: $resi_{\mathcal{B}} = intt(resi_{\mathcal{B}})$
9: $tmpi_{\mathcal{A}} = Bconc(\mathcal{B}, \mathcal{A})$
10: $resi_{\mathcal{A}} = resi_{\mathcal{A}} - ntt(tmpi_{\mathcal{A}})$

Algorithm 2 *hmult*

Input: $\mathbf{ct0} = (ct_{00}, ct_{01})_{\mathcal{A}}, \mathbf{ct1} = (ct_{10}, ct_{11})_{\mathcal{A}}$

Output: $\mathbf{res} = (res_0, res_1)_{\mathcal{A}}$

1: $x = ct_{00} * ct_{10}$
2: $y = ct_{00} * ct_{11} + ct_{01} * ct_{10}$
3: $z = ct_{01} * ct_{11}$
4: $\mathbf{w} = keyswitch(z, evk)$
5: $res_0 = x + \mathbf{w}_0$
6: $res_1 = y + \mathbf{w}_1$