Exercise (Security against partial double-opening). Let $\mathcal{C} = (\text{Gen}, \text{Com}, \text{Open})$ be commitment scheme and $\mathcal{H}$ be a collision resistant hash function family with an appropriate domain. Then we can build a list commitment scheme on top of the ordinary commitment scheme:

$$\text{Gen}^*$$

\begin{align*}
\text{pk} &\leftarrow \text{Gen} \\
h &\leftarrow \mathcal{H} \\
\text{return } (\text{pk}, h)
\end{align*}

$$\text{Com}^*_{\text{pk}, \mathcal{H}}(x_1, \ldots, x_\ell)$$

\begin{align*}
(c_i, d_i) &\leftarrow \text{Com}_\text{pk}(x_i), \ i \in \{1, \ldots, \ell\} \\
c_s &\leftarrow h(c_1, \ldots, c_\ell) \\
\text{return } (c, (c_1, \ldots, c_\ell, d_1, \ldots, d_\ell))
\end{align*}

where the decommitment procedure just verifies $c_s = h(c_1, \ldots, c_\ell)$ and restores $x_i \leftarrow \text{Open}_{\text{pk}}(c_i, d_i)$ for $i \in \{1, \ldots, \ell\}$. Prove that the commitment scheme is secure against partial double openings defined through the following security game $\mathcal{G}$

\begin{align*}
(\text{pk}, h) &\leftarrow \text{Gen}^* \\
(c_s, c_1, \ldots, c_\ell, \hat{c}_1, \ldots, \hat{c}_\ell) &\leftarrow \mathcal{A}(\text{pk}, h) \\
(i, d_i, \hat{d}_i) &\leftarrow \mathcal{A}(\text{pk}, h) \\
\text{if } c_s &\neq h(c_1, \ldots, c_\ell) \lor c_s \neq h(\hat{c}_1, \ldots, \hat{c}_\ell) \text{ then return } 0 \\
\text{return } \bot &\neq \text{Open}_\text{pk}(c_i, d_i) \neq \text{Open}_\text{pk}(\hat{c}_i, \hat{d}_i) \neq \bot
\end{align*}

provided that the base commitment is $(t, \varepsilon_1)$-binding and the hash function family is $(\ell, \varepsilon_2)$-collision resistant.

Solution. Intuitively, there are two possible ways how the adversary $\mathcal{A}$ can breach the security. First, the adversary $\mathcal{A}$ may find a double opening for the base commitment scheme $\mathcal{C}$. Second, the adversary $\mathcal{A}$ can breaking collision resistant hash function $h \in \mathcal{H}$.

Given the output $(c_s, c_1, \ldots, c_\ell, \hat{c}_1, \ldots, \hat{c}_\ell)$ is straightforward to decide whether the adversary found a hash collision or not. Namely, the collision occurs if $h(c_1, \ldots, c_\ell) = h(\hat{c}_1, \ldots, \hat{c}_\ell)$ and there exists $c_i \neq \hat{c}_i$. Thus, we can convert the original adversary $\mathcal{A}$ into two adversaries $\mathcal{A}_1$ and $\mathcal{A}_2$. The adversary $\mathcal{A}_1$ runs internally $\mathcal{A}$ and outputs $(c_s, c_1, \ldots, c_\ell, \hat{c}_1, \ldots, \hat{c}_\ell)$ only if the event Collision does not occur, otherwise it halts. The adversary $\mathcal{A}_2$ also runs internally $\mathcal{A}$ but continues only if the event Collision occurs. By the construction it is straightforward to note that

$$\Pr[\mathcal{G}^\mathcal{A} = 1] = \Pr[\mathcal{G}^{\mathcal{A}_1} = 1] + \Pr[\mathcal{G}^{\mathcal{A}_2} = 1]$$

and thus it is sufficient if we analyse the success of both adversaries separately.

Note that $\mathcal{A}_1$ can succeed only if $\mathcal{A}$ double opens some commitment value $c_i$, since it always outputs $c_i = \hat{c}_i$ for all $i \in \{1, \ldots, \ell\}$. More formally, let

$$\mathcal{Q}^B$$

\begin{align*}
\text{pk} &\leftarrow \text{Gen} \\
(c, d, \hat{d}) &\leftarrow \mathcal{B}(\text{pk}) \\
\text{return } \bot &\neq \text{Open}_\text{pk}(c, d) \neq \text{Open}_\text{pk}(c, \hat{d}) \neq \bot
\end{align*}

be the binding game. Then we can use the following a reduction construction $\mathcal{B}(\text{pk})$

\begin{align*}
h &\leftarrow \mathcal{H} \\
(c_s, c_1, \ldots, c_\ell, \hat{c}_1, \ldots, \hat{c}_\ell) &\leftarrow \mathcal{A}_1(\text{pk}, h) \\
(i, d_i, \hat{d}_i) &\leftarrow \mathcal{A}_1(\text{pk}, h) \\
\text{return } (c, d, \hat{d})
\end{align*}
By inlining the definition of $B$ into the game $Q$ we obtain a slightly modified game

$$G_1$$

$$\begin{align*}
&pk, \leftarrow \text{Gen}, h \leftarrow \mathcal{H} \\
&(c_*, c_1, \ldots, c_\ell, \hat{c}_1, \ldots, \hat{c}_\ell) \leftarrow A_1(pk, h) \\
&(i, d_i, \hat{d}_i) \leftarrow A_{\text{Com}}(pk, h) \\
&\text{return } \perp \neq \text{Open}_{pk}(c_i, d_i) \neq \text{Open}_{pk}(c_i, \hat{d}_i) \neq \perp
\end{align*}$$

which is more liberal compared to the original security game $G$ due to omitted tests. As a result, we get

$$\Pr[G_{A_1}^1 = 1] \leq \Pr[G_{A_1}^2 = 1] = \Pr[Q^B = 1] = \text{Adv}^{\text{bind}}_C(B).$$

Now note that the time needed to check whether the collision exists or not is $\Theta(\ell)$ and thus the running time of $A_1$ and $B$ is only $\Theta(\ell)$ bigger than the running time for $A$. Hence for $(t - O(\ell))$-time adversaries $A$, we can conclude that $\Pr[G_{A_1}^1 = 1] \leq \varepsilon_1$ if the commitment is $(t, \varepsilon_1)$-binding.

By the construction, $A_2$ can succeed only if $A_1$ finds a hash collision and thus its success is bounded by $\varepsilon_2$. Formally, we must still prove it by providing an explicit reduction to the collision-resistance game

$$G'$$

$$\begin{align*}
&h \leftarrow \mathcal{H} \\
&(m_1, m_2) \leftarrow B(h) \\
&\text{return } m_1 \neq m_2 \land h(m_1) = h(m_2).
\end{align*}$$

The reduction is trivial

$$B(h)$$

$$\begin{align*}
&pk \leftarrow \text{Gen} \\
&(c_*, c_1, \ldots, c_\ell, \hat{c}_1, \ldots, \hat{c}_\ell) \leftarrow A_2(pk, h) \\
&m_1 \leftarrow (c_1, \ldots, c_\ell) \\
&m_2 \leftarrow (\hat{c}_1, \ldots, \hat{c}_\ell) \\
&\text{return } (m_1, m_2).
\end{align*}$$

By inlining this adversary definition in to the game $Q$, we obtain a more liberal game

$$G_2$$

$$\begin{align*}
&pk, \leftarrow \text{Gen}, h \leftarrow \mathcal{H} \\
&(c_1, \ldots, c_\ell, \hat{c}_1, \ldots, \hat{c}_\ell) \leftarrow A_2(pk, h) \\
&\text{return } h(c_1, \ldots, c_\ell) = h(\hat{c}_1, \ldots, \hat{c}_\ell) \land (c_1, \ldots, c_\ell) \neq (\hat{c}_1, \ldots, \hat{c}_\ell)
\end{align*}$$

compared to the game $G$. Thus, we arrive at

$$\Pr[G_{A_2}^1 = 1] \leq \Pr[G_{A_2}^2 = 1] = \Pr[Q^B = 1] = \text{Adv}^{\text{cr}}_H(B).$$

Again, the overhead in the running-time of $B$ is $O(\ell)$ and thus for all $(t - O(\ell))$-time adversaries $A$, we can conclude that $\Pr[G_{A_2}^1 = 1] \leq \varepsilon_2$ if the hash function family is $(t, \varepsilon_2)$-collision resistant.