Let $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ be groups of order p and let $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ be the bilinear map. The IBE system works as follows.

Setup: The PKG picks random generators $p_1, g_1 \in \mathbb{G}_1$, generators $q_2, h_1, h_2, h_3 \in \mathbb{G}_2$ and a random $\alpha \in \mathbb{Z}_p$. It sets $g_1 = p_1^{\alpha} \in \mathbb{G}_1$. It chooses a hash function H_1 and $H_2 : \{0,1\}^* \to \{0,1\}^n$ from a family of universal one-way hash functions. The public *params* and private *masterkey* are given by

$$params = (p_1, q_2, h_1, h_2, h_3, H_1, H_2) \qquad masterkey = \alpha$$

KeyGen: To generate a private key for identity $\mathrm{ID} \in \mathbb{Z}_p$, the PKG generates random $r_{\mathrm{ID},i} \in \mathbb{Z}_p$ for $i \in \{1,2,3\}$, and outputs the private key

$$d_{\mathrm{ID}} = \{(r_{\mathrm{ID},i}, h_{\mathrm{ID},i}) : i \in \{1,2,3\}\}, \text{ where } h_{\mathrm{ID},i} = \left(h_i q_2^{-r_{\mathrm{ID},i}}\right)^{\frac{1}{\alpha - \mathrm{ID}}} \in \mathbb{G}_2$$

If $\mathrm{ID} = \alpha$, the PKG aborts. As before, we require that the PKG always use the same random values $\{r_{\mathrm{ID},i}\}$ for ID.

Encrypt: To encrypt $m \in \{1,0\}^n$ using identity $\mathrm{ID} \in \mathbb{Z}_p$, the sender generates random $s \in \mathbb{Z}_p$, and sends the ciphertext

$$\begin{aligned} C &= \left(g_1^s p_1^{-s\cdot \mathrm{ID}},\ e(p_1, q_2)^s,\ m \oplus H_2\{e(p_1, h_1)^s\},\ e(p_1, h_2)^s e(p_1, h_3)^{s\beta}\right) \\ &= (u, v, w, y) \end{aligned}$$

Note that $u \in \mathbb{G}_1, v \in \mathbb{G}_T, w \in \{1,0\}^n$ and $y \in \mathbb{G}_T$. We set $\beta = H_1\{u, v, w\}$. Encryption does not require any pairing computations once $e(p_1, q_2)$, and $\{e(p_1, h_i)\}$ have been pre-computed or alternatively included in *params*.

Decrypt: To decrypt ciphertext $C = (u, v, w, y)$ with ID, the recipient sets $\beta = H_1\{u, v, w\}$ and tests whether

$$y = e\left(u, h_{\mathrm{ID},2} h_{\mathrm{ID},3}^{\beta}\right) v^{r_{\mathrm{ID},2} + r_{\mathrm{ID},3}\beta}$$

If the check fails, the recipient outputs $\perp$. Otherwise, it outputs

$$m = w \oplus H_2\{e(u, h_{\mathrm{ID},1})\, v^{r_{\mathrm{ID},1}}\}$$

Correctness: Assuming the ciphertext is well-formed for ID:

$$\begin{aligned} &e\left(u, h_{\mathrm{ID},2} h_{\mathrm{ID},3}^{\beta}\right) v^{r_{\mathrm{ID},2} + r_{\mathrm{ID},3}\beta} \\ &\quad = e\left(p_1^{s(\alpha - \mathrm{ID})}, \left(h_2 h_3^{\beta}\right)^{\frac{1}{\alpha - \mathrm{ID}}} q_2^{\frac{-\left(r_{\mathrm{ID},2} + r_{\mathrm{ID},3}\beta\right)}{\alpha - \mathrm{ID}}}\right) e(p_1, q_2)^{s\left(r_{\mathrm{ID},2} + r_{\mathrm{ID},3}\beta\right)} \\ &\quad = e\left(p_1^{s(\alpha - \mathrm{ID})}, \left(h_2 h_3^{\beta}\right)^{\frac{1}{\alpha - \mathrm{ID}}}\right) = e(p_1, h_2)^s e(p_1, h_3)^{s\beta} \end{aligned}$$

Thus, the check passes. Moreover, as in the ANON-IND-ID CPA scheme,

$$e(u, h_{\mathrm{ID}})\, v^{r_{\mathrm{ID},1}} = e\left(p_1^{s(\alpha - \mathrm{ID})}, h^{\frac{1}{\alpha - \mathrm{ID}}} q_2^{\frac{-r_{\mathrm{ID},1}}{\alpha - \mathrm{ID}}}\right) e(p_1, q_2)^{s r_{\mathrm{ID},1}} = e(p_1, h)^s,$$

as required.