Anonymous Identity-Based Broadcast Encryption

Let k denote the security parameter given to the setup algorithm such that a security level of 256 bits is achieved. Let G be some BDH parameter generator.
Setup(k)***:*** Given a security parameter $k \in \mathbb{Z}^+$ the algorithm works as follows:

1. Run G on input k to generate a prime q, two groups $\mathbb{G}_1, \mathbb{G}_2$ of order q, and an admissibile bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. Choose a random generator $P \in \mathbb{G}$.

2. Pick a random $s \in \mathbb{Z}_q^*$ and set $P_{pub} = sP$

3. Choose a cryptographic hash function $H_1 : \{0,1\}^* \to \mathbb{G}_1^*$. The security analysis will view H_1 as a random oracle.

The symmetric key space is $K = \{0,1\}^{256}$. The ciphertext space is $C_i = \mathbb{G}_1^* \times \{0,1\}^{256}$
Extract: For a given

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

If 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 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:

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

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

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

as required.