## Anonymous Identity-Based Broadcast Encryption Scheme

We let $\lambda$ be the security parameter given to the setup algorithm such that a security level of 256 bits is realised. We let $G$ be some BDH parameter generator. $S$ is the set of desired recipients $i$ with $i = 1, .., n$. Symmetric encryption and decryption is done using AES Galois Counter Mode $GCM_{enc}(P, A, K, IV)$ and $GCM_{dec}(P, A, K, IV)$ respectively.

***Setup***$(\lambda)$***:*** Given a security parameter $\lambda \in \mathbb{Z}^+$, the algorithm works as follows:

1. Run $G$ on input $\lambda$ to generate a prime $q$, two groups $\mathbb{G}_1, \mathbb{G}_2$ of order $q$, and an admissible bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. Choose a random generator $P \in \mathbb{G}_1$
2. Pick a random $s \in \mathbb{Z}_q^*$ and set $P_{pub} = sP$
3. Choose cryptographic hash functions $H_1 : \{0,1\}^* \to \mathbb{G}_1^*$, $H_2 : \mathbb{G}_T^* \to \{0,1\}^{256}$, $H_3 : \{0,1\}^{256} \to \{0,1\}^{256}$ and $H_4 : \{0,1\}^{256} \to \{0,1\}^{256}$. The security analysis will view $H_1, H_2$ as random oracles.

The symmetric key space is $K = \{0,1\}^{256} = \{K_1||IV\}$ with $K_1 = \{0,1\}^{128}$ and $IV = \{0,1\}^{128}$. The ciphertext space is $C_i = \mathbb{G}_1^* \times \{0,1\}^{256}$. The system parameters are $params = \{q, \mathbb{G}_1, \mathbb{G}_2, e, P, P_{pub}, H_1, H_2\}$. The master key is $s \in \mathbb{Z}_q^*$.

***KeyGen***$(\lambda, ID_i)$***:*** For a given string $ID_i \in \{0,1\}^*$ the algorithm does:

1. Compute $Q_{\mathrm{ID}_i} = H_1(ID_i)$
2. Set the private key $d_{\mathrm{ID}_i}$ to be $d_{\mathrm{ID}_i} = sQ_{\mathrm{ID}_i}$ where $s$ is the master key.
3. Return $d_{\mathrm{ID}_i}$ to the corresponding user $ID_i$ over a secure channel.

***Encrypt***$(params, \lambda, K, S)$***:*** To encrypt $K$ under the public keys $\{ID_i \in S\}$:

1. Generate a random symmetric session key $K_1 = \{0,1\}^{128}$. Generate a random initialisation vector $IV = \{0,1\}^{128}$ and set $K = \{K_1||IV\}$
2. Choose a random $\sigma \in \{0,1\}^{256}$ and set $r = H_3(\sigma, K)$
3. For each recipient $ID_i \in S, i = 1..n$, calculate the ciphertext
$$W_i = \sigma \oplus H_2\left(g_{\mathrm{ID}_i}^r\right) \quad \text{where} \quad g_{\mathrm{ID}_i} = e\left(Q_{\mathrm{ID}_i}, P_{pub}\right) \in \mathbb{G}_T^*$$
4. Apply GCM with initialisation vector $IV$ and secret key $K_1$. Plaintext $P_{text}$ is the message to be broadcasted and the additional authenticated data:
$$\begin{aligned} A &= \{n||rP||K \oplus H_4(\sigma)||W_1||W_2||..||W_n||P_{text}\} \\ &= \{n||U||V||W\} \quad \text{where} \quad W = \{W_1||W_2||..||W_n\} \end{aligned}$$
GCM then outputs a ciphertext $C_T$ and an authentication tag $T$ such that
$$\{C_T, T\} = GCM_{enc}(P_{text}, A, K_1, IV)$$
5. The following message is then broadcasted over an insecure network
$$M = \{A||T||C_T\}$$

***Decrypt***$(params, d_{ID_i}, M)$**:** Parse broadcasted message $M$ as $\{n||U||V||W||T||C_T\}$. For each $W_i \in W$ do the following:

1. Decrypt $\sigma$ using the private key $d_{\mathrm{ID}_i}$ by calculating $W_i \oplus H_2\left(e\left(d_{\mathrm{ID}_i}, U\right)\right) = \sigma$
2. Compute $V \oplus H_4\{\sigma\} = K$
3. Set $r = H_3\left(\sigma, K\right)$. Test that $U = rP$. If not, try next $W_i$ and return to 1.
4. Decrypt $C_T$ by

$$\{P_{text}, T_{dec}\} = GCM_{dec}\left(C_T, A, K_1, IV\right)$$

5. Verify whether $T_{dec}$ corresponds to $T$ in $M$.
   If $T \neq T_{dec}$, return $\perp$. Output $P_{text}$ as the broadcasted message otherwise.