single round, n-party key agreement based on multi-TA WIBE coalition techniques

(Boneh-Boyen mTA WIBE)

$\boxed{\text{Parameters}}$ $g_1, u, v \xleftarrow{\$} \mathbb{G}_1$

Hash $g_2 \xleftarrow{\$} \mathbb{G}_2$

$H: \mathbb{IP} \to \mathbb{Z}/p\mathbb{Z}$

$e: \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$
(Bilinear)

n parties:
$TA_1, TA_2, \ldots, TA_n$

w/ n public keys
$t_1, t_2, \ldots, t_n$

w/ n private keys
$s_1, s_2, \ldots, s_n$

such that $s_i = g_2^{k_i}$ & $t_i = g_1^{k_i}$

Note: $|\mathbb{G}_1| = |\mathbb{G}_2| = p$

Each TA_i chooses

$$r_{ij} \xleftarrow{\$} \mathbb{Z}/p\mathbb{Z}$$

and publishes

$$\boxed{d_{ij} = \left(s_i \left(uv^{H(TA_j)}\right)^{r_{ij}}, g_1^{r_{ij}}\right)}$$

TA_i also chooses $a_i, b_i \xleftarrow{\$} \mathbb{Z}/p\mathbb{Z}$ and publishes ciphertext

$$C_{i1} = g_1^{b_i}$$

$$C_{i2} = (u^{b_i}, v^{b_i})$$

$$C_{i3} = e(g_1, g_2)^{a_i} \cdot e(\prod r_i, g_2)^{b_i}$$

TA_j combines the d_{ij} w/ S_j to get a coalition-compatible decryption key:

$$\tilde{S}_j = \left(S_j \prod s_i \left(u v^{H(TA_j)} \right)^{r_{ij}}, \prod g_1^{r_{ij}} \right)$$

$$\tilde{S}_j = \left(g_2^{\Sigma k_i} \left(u v^{H(TA_j)} \right)^{\Sigma r_{ij}}, g_1^{\Sigma r_{ij}} \right)$$

Each TA_j may then decrypt each ciphertext individually and combine the messages under multiplication to recover $e(g,g)^{\sum a_i}$

— OR —

decrypt the product of the ciphertexts to get the same result using only two pairings