Kolonelos-Malavolta-Wee construction: distributing BGW

pp: $(g, g_1, g_2, \dots, g_N, g_{N+2}, \dots, g_{2N})$ where $g_i = g^{\alpha^i}$

To generate a public/secret key-pair for index $i \in [N]$, user chooses $\gamma_i \xleftarrow{R} \mathbb{Z}_p$ and first sets

$$sk_i = (g_i, g_i^{\gamma_i}) \qquad pk_i = g^{\gamma_i}$$

analog of master public key $v = g^{\gamma}$

How to encrypt to a set $S \subseteq [N]$?

Let public keys be $\{pk_j\}_{j \in S} = \{g^{\gamma_j}\}_{j \in S}$

Define the aggregate public key for the set S to be $\prod_{j \in S} g^{\gamma_j} = g^{\sum_{j \in S} \gamma_j}$

and encrypt as if $mpk = v_S = \prod_{j \in S} g^{\gamma_j}$

Ciphertext is as in BGW with v_S as mpk:

$$g^r, \quad \left[v_S \cdot \prod_{j \in S} g_{N+1-j}\right]^r, \quad e(g, g_N)^r \cdot m$$

To decrypt, user j needs to "help" by providing "cross terms"

User j includes $g_1^{\gamma_j}, g_2^{\gamma_j}, \dots, g_{j-1}^{\gamma_j}, g_{j+1}^{\gamma_j}, \dots, g_N^{\gamma_j}$ as part of its public key.

Main decryption components for user i:

$$e(g_i, ct_2) = e\Big(g_i, v_S \cdot \prod_{j \in S} g_{N+1-j}\Big)^r$$

$$= e(g_i, v_S)^r \, e(g, g_{N+1})^r \prod_{j \in S \setminus \{i\}} e(g, g_{N+1-j+i})^r$$

$$e\Big(g_i^{\gamma_i} \cdot \prod_{j \in S \setminus \{i\}} g_{N+1-j+i}, ct_1\Big) = e(g_i^{\gamma_i}, g)^r \prod_{j \in S \setminus \{i\}} e(g, g_{N+1-j+i})^r$$

ratio gives $\underbrace{e(g, g_{N+1})^r}_{\text{KEM}} \cdot \dfrac{e(g_i, v_S)^r}{e(g_i^{\gamma_i}, g)^r}$

$$= e(g, g_{N+1})^r \cdot \prod_{j \in S \setminus \{i\}} e(g, g_i^{\gamma_j})^r$$

part of user j's public key