Kolos-Malavolta-Wee construction: distributing BGW

\[ pp = (g, g_1, g_2, \ldots, g_n, g_{N+2}, \ldots, g_{2N}) \quad \text{where} \quad g_i = g^i \]

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

\[ S_k = (g_i, g_i^y) \quad \text{pk}_i = g_i^y \]

\[ \text{analog of master public key} \quad v = g^y \]

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

Let public keys be \( \{ \text{pk}_j \}_{j \in S} = \{ g_j^y \}_{j \in S} \)

Define the aggregate public key for the set \( S \) to be

\[ g = \prod_{j \in S} g_j^y = g \sum_{j \in S} y_j \]

and encrypt as if \( \text{mpk} = v_S = \prod_{j \in S} g_j^y \)

Ciphertext is as in BGW with \( v_S \) as mpk:

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

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

User \( j \) includes \( g_j^y, g_{N-j}^y, \ldots, g_{N-1}^y, g_N^y, \ldots, g_j^y \) as part of its public key.
Main decryption components for user $i$:

\[
\begin{align*}
    e(g_i, c_{t_2}) &= e\left(g_i, vs \cdot \prod_{j \in s} g_{N+1-j}\right)^r \\
    &= e(g_i, vs)^r e\left(g, g_{N+1}\right)^r \prod_{j \in s\setminus i} e\left(g, g_{N+1-j+i}\right)^r \\
    e\left(g_i^\gamma, \prod_{j \in s\setminus i} g_{N+1-j+i}, c_{t_1}\right) &= e\left(g_i^\gamma, g\right)^r \prod_{j \in s\setminus i} e\left(g, g_{N+1-j+i}\right)^r \\
\end{align*}
\]

\[\xrightarrow{\text{ratio gives}} \quad \frac{e(g_i, vs)^r}{e(g_i^\gamma, g)^r} \quad \frac{e(g_i, vs)^r}{e(g_i^\gamma, g)^r} \quad \xrightarrow{\text{KEM}} \]

\[
= e\left(g, g_{N+1}\right)^r \cdot \prod_{j \in s\setminus i} e\left(g, g_j^\gamma\right)^r
\]

\[\xrightarrow{\text{part of user } j\text{'s public key}}\]