\textbf{Input: } $\phi_m$ such that $\sum_{m=1}^{M} \phi_m = 0$

\textbf{Service Provider}

- Receives $[\psi_{(m,r)}]_H$ for $r \in \{1, \ldots, R\}$ and $m \in \{1, \ldots, M\}$

\textbf{User $i$}

\[ [\tilde{D}_i^2]_H \] for $i \in G_m$

- Decryps: $[\tilde{D}_i^2]_H$

- Encrypts: $\gamma_{(i,j)}$ for $j \in \{1, \ldots, K\}$

\[ [\gamma_{(i,j)}]_H \text{ for } j \in \{1, \ldots, K\} \]

- Computes: $[\tilde{\Gamma}_i]_H$

\[ [\tilde{S}_{(i,r)}]_H \text{ for } r \in \{1, \ldots, R\} \]

- Computes: $[\tilde{S}_{(i,r)}]_H$

- Generates: $\alpha_m$ and $\beta_{(m,r)}$

\[ [\tilde{\Gamma}_m + \alpha_m]_H, [\tilde{P}_{\Sigma(m,r)} + \beta_{(m,r)}]_H \]

- Decryps: $[\tilde{\Gamma}_m + \alpha_m]_H$ and $[\tilde{P}_{\Sigma(m,r)} + \beta_{(m,r)}]_H$

- $\tilde{\Gamma}_m + \alpha_m + \phi_m, \tilde{P}_{\Sigma(m,r)} + \beta_{(m,r)} + \psi_{(m,r)}$

- Computes: $\tilde{P}_{\Sigma}$ and $\tilde{\Gamma}_\Sigma$