

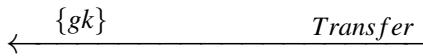
Uploading

1. System Parameter Generation

$$\lambda = (f(\cdot), h(\cdot), q)$$

2. Key Generation

Keep the KEY MATCHING Table

**3. Index Generation and Document Encryption**

$$\xrightarrow{\{f_{gk_i^j}(d_n), f_{gk_i^j}(D_n), f_{gk_i^j}(w_{n,1}), f_{gk_i^j}(w_{n,2}), \dots\}}$$

4. Database Update*Decrypt → Re-encrypt;*

$$\xrightarrow{\{f_{k_c}(d_n), f_{dk_i}(D_n), f_{ik_i}(w_{n,1}), \dots\}} \text{Insert to Database}$$

Downloading

1. Trapdoor Generation

$$\xrightarrow{\{g_i, f_{gk_i^j}(w)\}} \text{Decrypt} \rightarrow \text{Re-encrypt};$$

$$\xrightarrow{T_w=f_{ik_i}(w)}$$

2. Retrieval

Index List

Encrypted Document

Return;

$$\text{Decrypt} \rightarrow \text{Re-encrypt}; \qquad \xleftarrow{\{f_{dk_i}(D_t)\}}$$

$$\xleftarrow{\{f_{gk_i^j}(D_t)\}}$$

3. Decryption $\{D_t\}$