| *User* | *GM* | *DS* |
|---|---|---|
| Uploading | | |
| | **1. System Parameter Generation** | |
| | $\lambda = (f(\cdot),\ h(\cdot),\ q)$ | |
| | **2. Key Generation** | |
| | Keep the KEY MATCHING Table | |
| $\{gk\}$ ← | $Transfer$ | |
| **3. Index Generation and Document Encryption** | | |
| $\{f_{gk_i^j}(d_n), f_{gk_i^j}(D_n), f_{gk_i^j}(w_{n,1}), f_{gk_i^j}(w_{n,2}), \ldots\}$ → | | |
| | **4. Database Update** | |
| | $Decrypt \rightarrow Re-encrypt;$ | |
| | $\{f_{k_c}(d_n), f_{dk_i}(D_n), f_{ik_i}(w_{n,1}), \ldots\}$ → | Insert to Database |
| Downloading | | |
| **1. Trapdoor Generation** | | |
| $\{g_i,\ f_{gk_i^j}(w)\}$ → | $Decrypt \rightarrow Re-encrypt;$ | |
| | $T_w = f_{ik_i}(w)$ → | **2. Retrieval** |
| | | Index List |
| | | Encrypted Document |
| | | Return; |
| | $Decrypt \rightarrow Re-encrypt;$ | $\{f_{dk_i}(D_t)\}$ ← |
| **3. Decryption** | $\{f_{gk_i^j}(D_t)\}$ ← | |
| $\{D_t\}$ | | |