Problem Statement

- Verifiable Attribute-Based Search over Shared Cloud Data
  - Cloud data engines provide information search services on behalf of data owner.
  - The correctness of search results cannot be guaranteed if the SP tampers with data records deliberately.
  - Users might be curious about inaccessible data, which motivates to protect data access against unauthorized users.

- Threat Model
  - Users need to ensure the integrity of query results from the following two perspectives:
    - Soundness: No records in results are tampered with and are truly the results with respect to their own roles.
    - Completeness: All records in results are either non-results or inaccessible to users.
  - Data are cryptographically enforced with fine-grained access control.
  - Data content and access policy are protected in a zero-knowledge manner.

vABS Architecture

- Verifiable attribute-based search services over shared cloud data.
- Client side: attribute-based search and result verification.
- Server side: query processing and VO construction.

Verifiable Equality Search

- Introduce a global pseudo access role $Role_{do}$, which is not possessed by any user.
- Treat non-existent data records as the data records that cannot be accessed by any user.
- Therefore, a data record is either accessible or inaccessible to the query user.

- ADS Generation and Query Processing
  - APP Signature: $\sigma_i$ data content $v_i$, access policy $T$, and is signed by the data owner for ADS generation.
    $$\sigma_i = \text{APS.Sign}(sk_{do}, hash(v_i), hash(T))$$
  - APS Signature: $\tilde{\sigma}_{a} = \text{ABS.Sign}(sk_{do}, hash(a_i), hash(v_i), T_a)$
    $$\tilde{\sigma}_{a} = \text{ABS.Sign}(sk_{do}, hash(a_i), hash(v_i), T_a)$$

- Query results and VO are encrypted with CP-ABE before sending to the users to prevent impersonation attacks.

Verifiable Search Range

- Access-Policy-Preserving Grid-Tree
  - Non-Leaf Node:
    - Access policy $p_i = p_{i_1} \lor p_{i_2} \lor \cdots \lor p_{i_n}$
    - APP signature $\tilde{s}_{i} = \text{ABS.Sign}(sk_{do}, \phi_{i}, p_i)$
  - Leaf Node: Access policy and APP signature are identical to those of underlying data.
  - Relaxing Zero-Knowledge Requirement

Demonstration

Reference