• Generic Construction of Attribute-Based Encryption from Public-Key Searchable Encryption

Previous research

Attribute-Based Encryption → Generic construction → Searchable Encryption

Not given rigorous proofs

Our research

Key-Policy Attribute-Based Encryption → Propose a generic construction → Public-Key Searchable Encryption

IND-CPA and IND-ANO-IND-CPA

• Cryptography with Advanced Functionality

Public-Key Encryption

Cloud service

Searchable Encryption

Add functionality

pk

sk

sk_1
Engineering, 3rd grade std

sk_2
Literature, 3rd grade std

sk_3
Engineering, 4th grade std

3rd grade std

Attribute-Based Encryption

Cryptography with Advanced Functionality