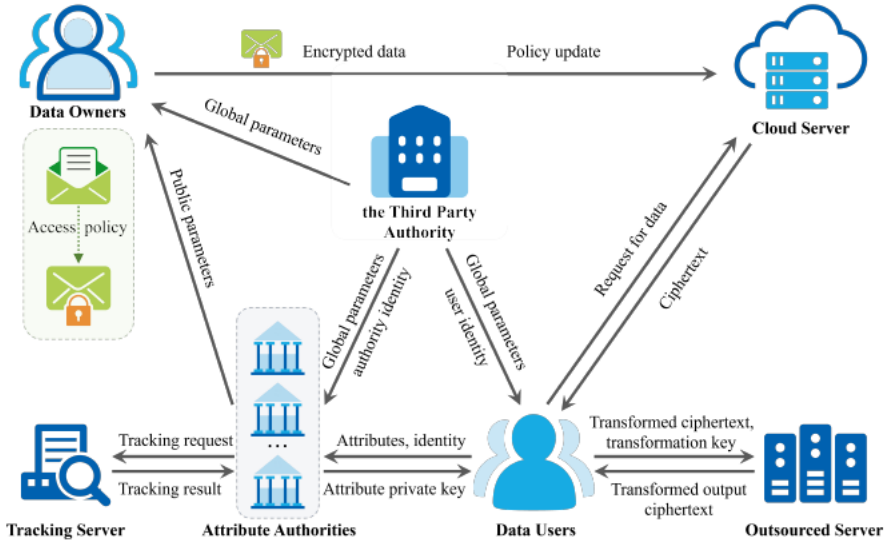
Traceable and revocable multi-authority ABE supporting decryption outsourcing and policy update for cloud data access control

Yanqing YAO, Yunjia ZHANG, Zhiyi LIU, Yuxuan WANG, Xinyu TAN, Zhengde ZHAI

Frontiers of Computer Science, DOI: 10.1007/s11704-025-41356-7

Problems & Ideas

- Problems of conventional attribute-based encryption approaches:
  - The issues of collusion among authorities, excessive decryption computation overhead, and high complexity in ABE have aroused attention.
  - Expanding the functionality of ABE to satisfy multiple requirements and improving existing functionality of ABE schemes are still urgent problems.
- Ideas: A novel ABE scheme that incorporates functional features such as multi-authority key generation, malicious user tracking, flexible attribute revocation, and real-time policy updates.



System model of the multi-functional MA-ABE scheme for cloud data access control.

Main Contributions

- Contributions:
  - A multi-functional multi-authority ABE data sharing model which provides improved privacy protection and effectively meets real needs;
  - A novel multi-functional multi-authority ABE scheme that incorporates functional features such as multi-authority key generation, outsourced decryption, malicious user tracking, flexible attribute revocation, and real-time policy updates;
  - Our scheme can resist collusion attacks while maintaining static and forward security; our scheme can significantly improve time efficiency, reduce key size, and shorten ciphertext length compared to known schemes, effectively decreasing the computation and storage costs.

Scheme	Multi-authority	Outsourcing Decryption	Attribute Revocation	Policy Update	Traceability
[15]	×	✓	×	×	×
[18]	✓	✓	×	✓	✓
[19]	✓	×	×	×	×
[30]	×	✓	✓	×	×
[41]	✓	×	×	×	✓
[42]	×	✓	×	×	✓
Our scheme	✓	✓	✓	✓	✓

Scheme	Public key size	Private key size	Ciphertext size	Number of bilinear pairings in decryption
[15]	$\|U_u\|+1$	$2\|S\|+3$	$3l+1$	$3\|I\|+2$
[18]	$4\|U_{AA}\|$	$4\|S\|+1$	$5l+1$	$4\|I\|$
[19]	3	$2\|U\|+2$	$\|U\|+3$	$2\|U\|+1$
[41]	$4\|U_{AA}\|$	$4\|S\|+1$	$6l+1$	$3\|I\|$
[42]	7	$2\|S\|+4$	$3l+3$	$3\|I\|+1$
Our scheme	$2\|U_{AA}\|$	$2\|S\|+1$	$4l+1$	$3\|I\|$

Comparisons of our scheme with several existing ABE access control schemes from the perspectives of functionalities and performance. Left: functionality comparison of our scheme with prior related works; Right: efficiency comparison of our scheme with prior related works