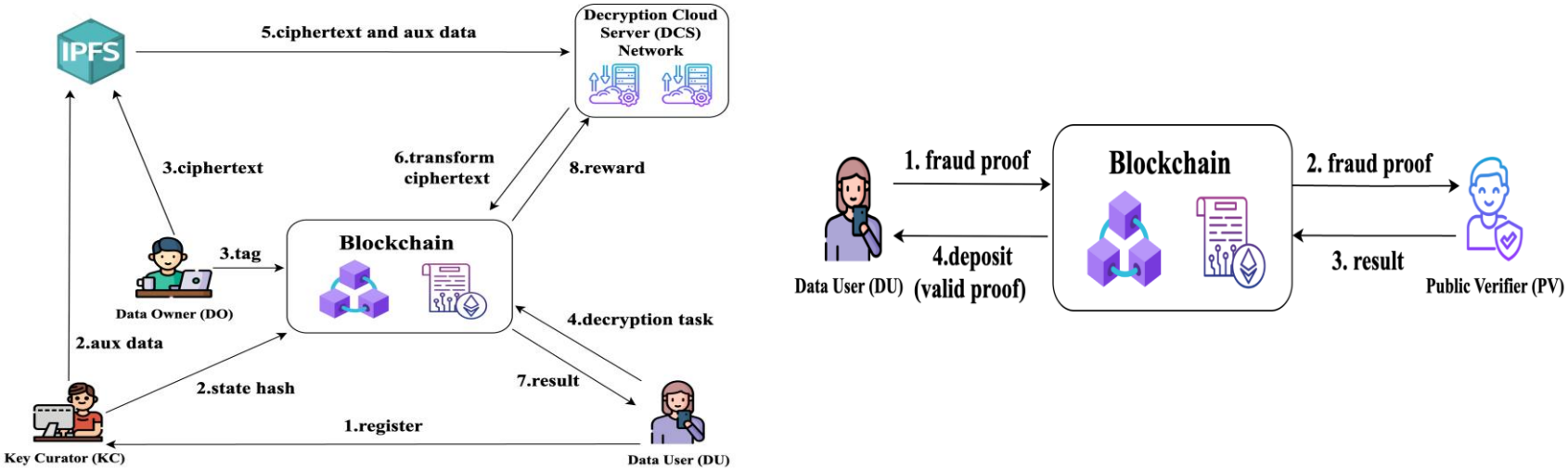
Registered Attribute-Based Encryption with Reliable Outsourced Decryption Based on Blockchain

Dongliang CAI, Liang ZHANG, Borui CHEN, Haibin KAN

Frontiers of Computer Science, DOI: 10.1007/s11704-025-50707-3

Problems & Ideas

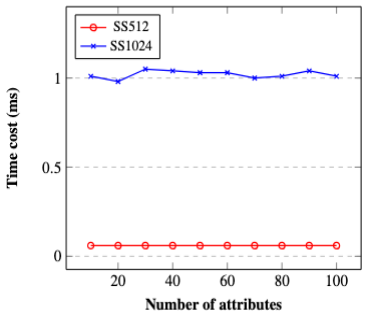
- Problems of decentralized and fine-grained data sharing:
  - Key escrow problem in attribute-based encryption (ABE);
  - Lack of reliable and efficient outsourced decryption for ABE;
  - No existing outsourced decryption scheme for registered ABE.
- Ideas: We address key escrow problem in decentralized data sharing using registered ABE and design an efficient and reliable outsourced decryption solution to making it friendly for user-centric lightweight devices.



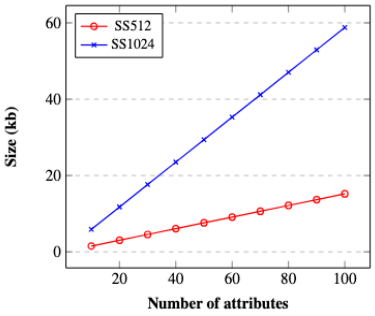
Overview of data sharing framework.
Left: optimistic case; Right: dispute case with fraud proof.

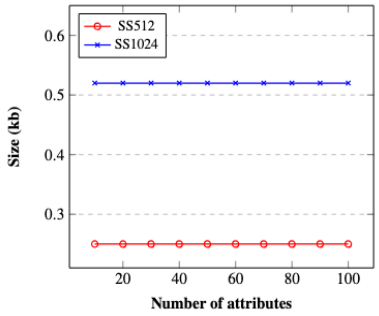
Main Contributions

- Contributions:
  - We propose the first registered ABE scheme with reliable outsourced decryption based on blockchain.
  - We achieve verifiability by a verifiable tag mechanism and ensure exemptibility through NIZK proof.
  - We propose a decentralized and auditable data sharing framework without a trusted authority. The reliable outsourced decryption makes it friendly for user-centric lightweight devices.
  - We give a concrete security analysis and implement on Ethereum to demonstrate feasibility and performance.

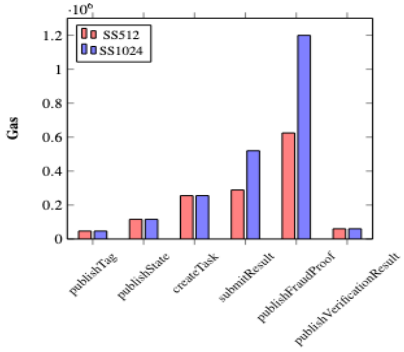


Fast Decryption





Small Transform Ciphertext Size
Left: original ciphertext; Right:transform ciphertext



Low and Constant Gas