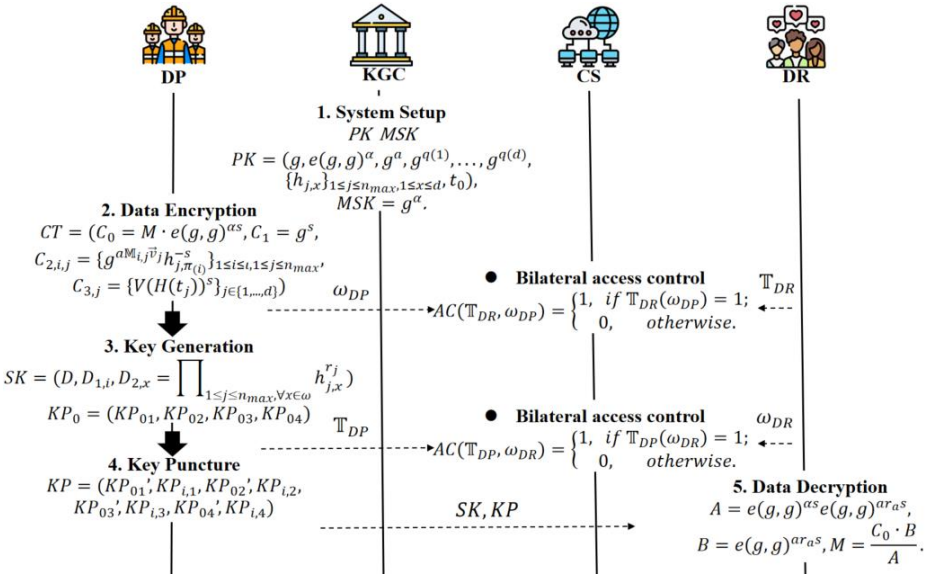
Towards Secure and Fine-grained Data Sharing over Cloud Platform

Fuyuan SONG, Xiaowei SUN, Yunlong GAO, Qin JIANG, Zhangjie FU

Frontiers of Computer Science, DOI: 10.1007/s11704-024-40279-z

Problems & Ideas

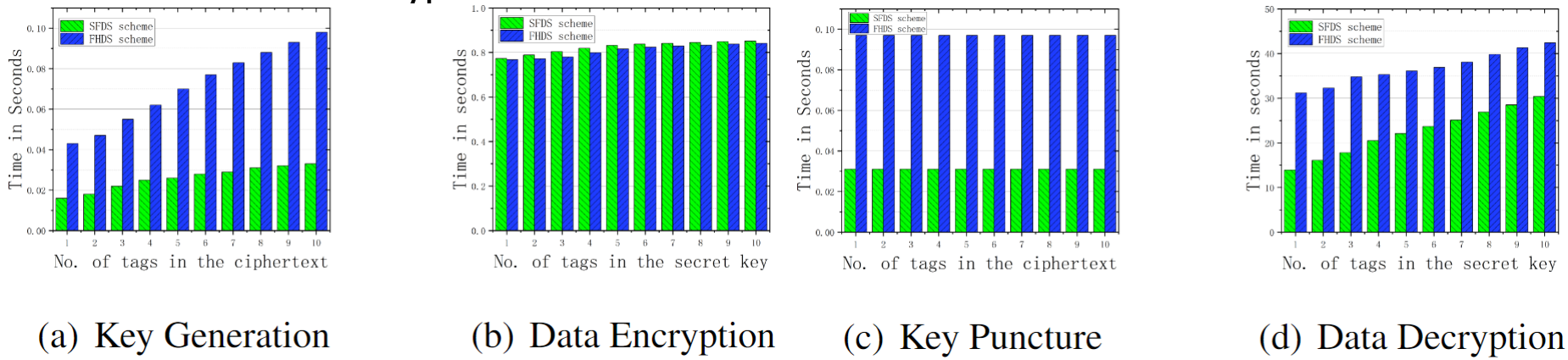
- Problems of data sharing over cloud platform:
  - Existing access control policies only focus on unilateral access control of data requesters, potentially failing to prevent unauthorized individuals from maliciously publishing data.
  - Existing key update schemes rely on trusted key generation centern (KGC) and have significant performance limitations.
- Ideas: We propose a Secure and Fine-Grained Data Sharing (SFDS) scheme with bilateral access control and non-interactive key update.



Workflow of SFDS. It shows five phases in the proposed SFDS scheme, including the detailed construction of each algorithm.

Main Contributions

- Contributions:
  - We propose an attribute-based encryption bilateral access control strategy that enables DP and DR to design access policies for secure data sharing and access.
  - We propose a key update mechanism based on puncturable encryption, allowing DP to non-interactively update their secret keys with out the need for the KGC.
  - The experimental evaluation demonstrates that SFDS outperforms the state-of-the-art scheme in terms of key generation, key puncture, and data decryption.



(a) Key Generation (b) Data Encryption (c) Key Puncture (d) Data Decryption

Computational cost of each algorithm. From Left to Right: The running time of key generation, data encryption, key puncture, data decryption with different number of tags in the ciphertext, respectively.