A Survey on Federated Learning: A Perspective from Multi-Party Computation

Fengxia LIU, Zhiming ZHENG, Yexuan SHI, Yongxin TONG, Yi ZHANG

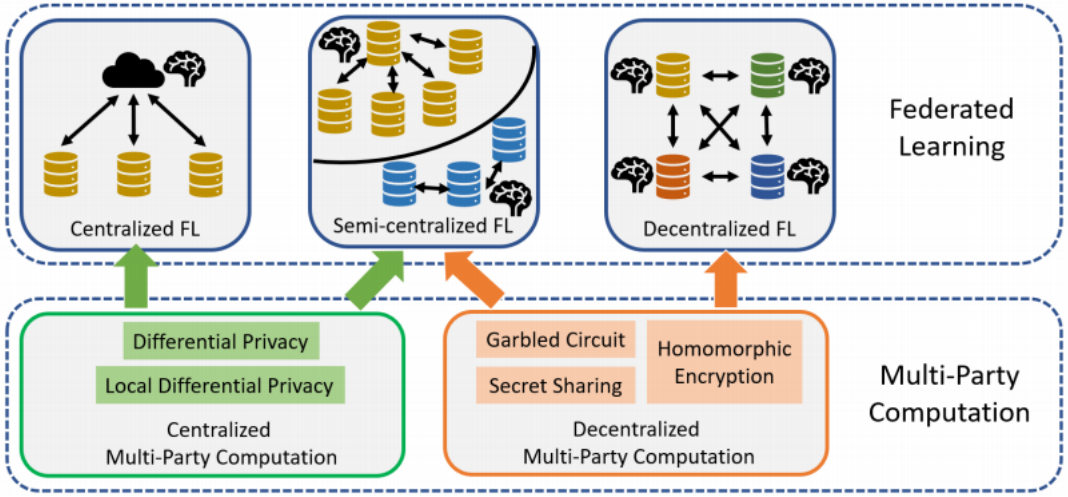
Frontiers of Computer Science, DOI: 10.1007/s11704-023-3282-7

Problems & Ideas

- Problems of Federated Learning:

  exchanging intermediate results e.g.,gradients rather than raw datasets may still leak privacy

- Ideas: Of our particular interest is multi-party computation, a generic and fundamental category of techniques that takes multi-party private inputs for aggregated computation without revealing the private data of each party.



The taxonomy of federated learning from a perspective of multi-party computation.

Main Contributions

- Contributions:
  - We review which multi-party computation schemes are suited for privacy protection in centralized, decentralized, and semi-centralized federated learning.
  - We also discuss how to improve the accuracy and efficiency of federated learning when adopting diverse multiparty computation techniques.

Summary of federated learning from a perspective of multi-party computation.

Federated Learning	Multi-Party Computation	Literature
Centrailized FL	Central Differential Privacy	[17], [18], [19], [20], [21], [40], [41] [42], [43], [44], [45], [46], [49]
	Local Differential Privacy	[7], [50], [52], [53], [54]
Decentralized FL	Garbled Circuit and Secret Sharing	[8], [15], [22], [66], [67], [69]
	Homomorphic Encryption	[22], [70], [71], [72]
Semi-centralized FL	/	[9], [10], [11], [82]