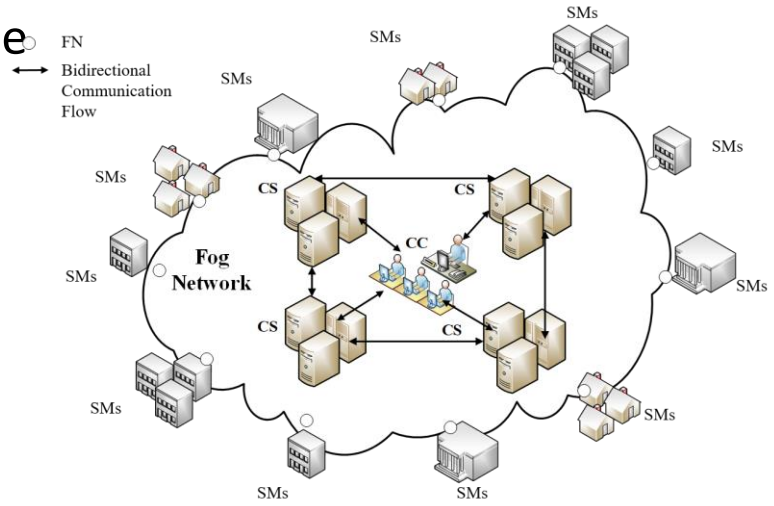
A Verifiable Privacy-Preserving Data Collection Scheme Supporting Multi-Party Computation in Fog-Based Smart Grid

Zhusen LIU, Zhenfu CAO, Xiaolei DONG, Xiaopeng ZHAO, Haiyong BAO, Jiachen SHEN

Frontiers of Computer Science, DOI: 10.1007/s11704-021-0410-0

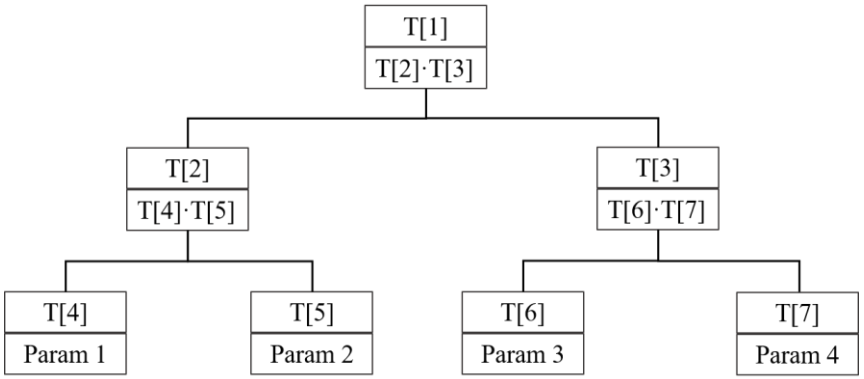
Problems & Ideas

- Problems of protecting privacy and data collection sccheme in smart grid
  - of great benefit to accept low-latency fog computing
  - mainly focus on secure additive data aggregation without taking other secure data analysis into consideration
  - not ensure the correctness of shares of participants during distribution and reconstruction in the data collection scheme supporting Multi-Party Computation (MPC)
- Ideas: Verifiable Secret Sharing Supporting MPC
  - Practical and Efficient Encryption Scheme
  - Verifiable Secret Sharing Scheme
  - Batch Verification of the Secret Shares



Main Contributions

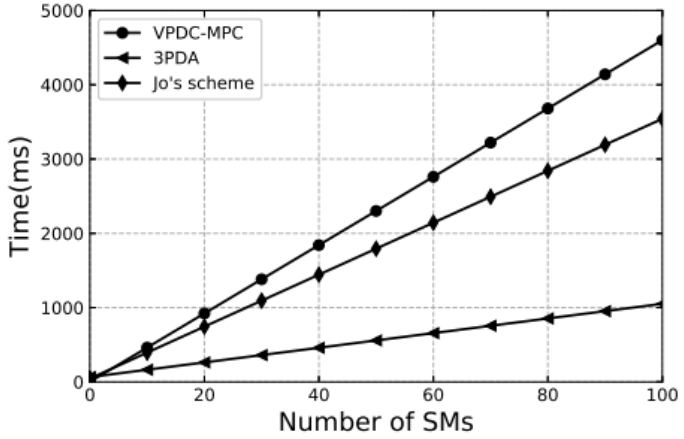
- Batch Verification of Secret Shares to Detect Error



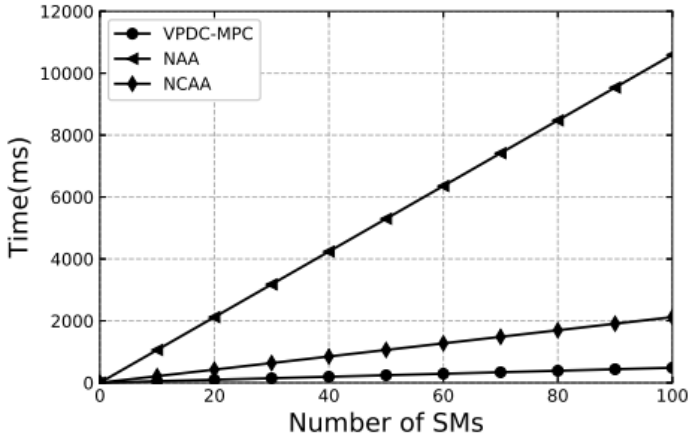
- Practical and Efficient Encryption Scheme

Comparison of Computation Cost of Encryption Schemes

	VPDC-MPC	3PDA	Jo's Scheme
Comp. Cost	12.1 ms	49.3 ms	45.07 ms



(a) Each FN



(b) Each CS

Computational Cost Comparison