

A novel privacy preserving data  
aggregation scheme with data  
integrity and fault tolerance for  
smart grid communications

**Haiyong BAO, Beibei LI**

Frontiers of Computer Science, DOI: [10.1007/s11704-020-9402-8](https://doi.org/10.1007/s11704-020-9402-8)

# Problems & Ideas

- Problems of design secure data aggregation scheme for smart grid communications

- achieving privacy preservation
- ensuring data integrity
- with fault tolerance property

- Ideas: Achieve privacy preservation,

data integrity, and fault tolerance simultaneously

- Based on the pre-calculated auxiliary information, a novel fault tolerant mechanism is designed
- A novel efficient authentication technique is proposed to achieve data integrity and source authentication
- According to the performance analysis, the proposed scheme outperforms the state-of-the-arts



