Traceable Ring Signature Schemes Based on SM2 Digital Signature Algorithm and Its Applications in the Data Sharing Scheme

Yongxin ZHANG, Hong LEI, Bin WANG, Qinghao WANG, Ning LU, Wenbo SHI, Bangdao CHEN, Qiuling YUE

Frontiers of Computer Science, DOI: 10.1007/s11704-023-3318-z

Problems & Ideas

- Problems of conventional data sharing approaches:
  - Strong privacy protections hinder regulation.
  - Conditional privacy protection relys on centralized trust.
- Ideas: An SM2-based traceable ring signature are employed in the data sharing model to enable the tracing without centralized trust.

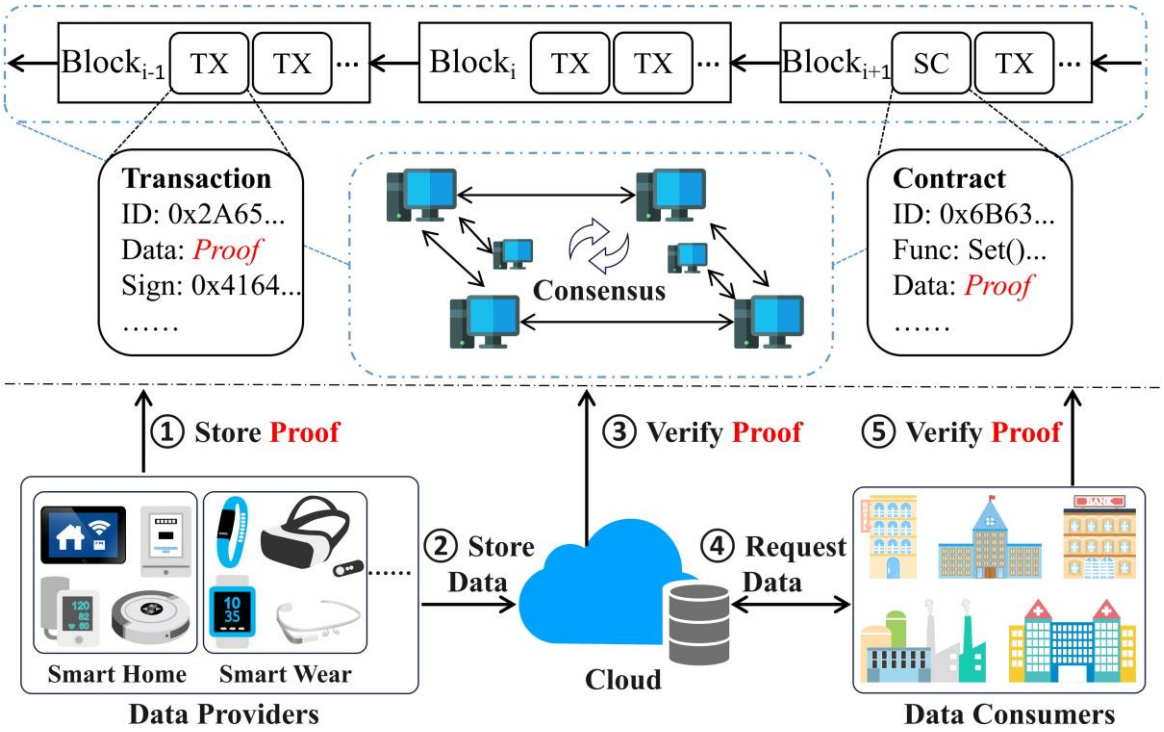
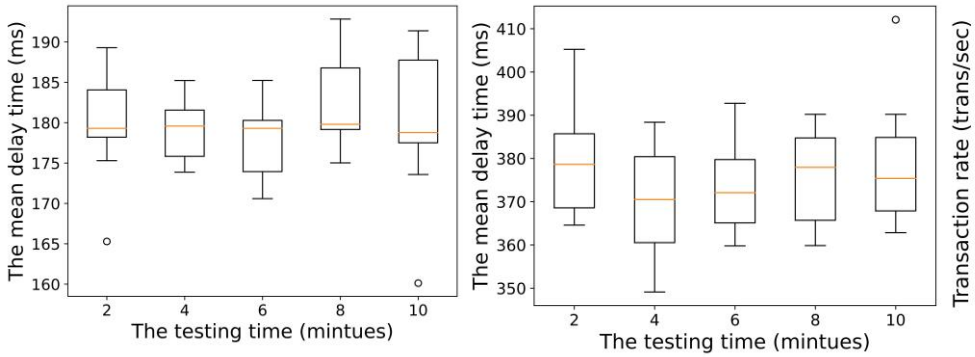


Fig.1 System model

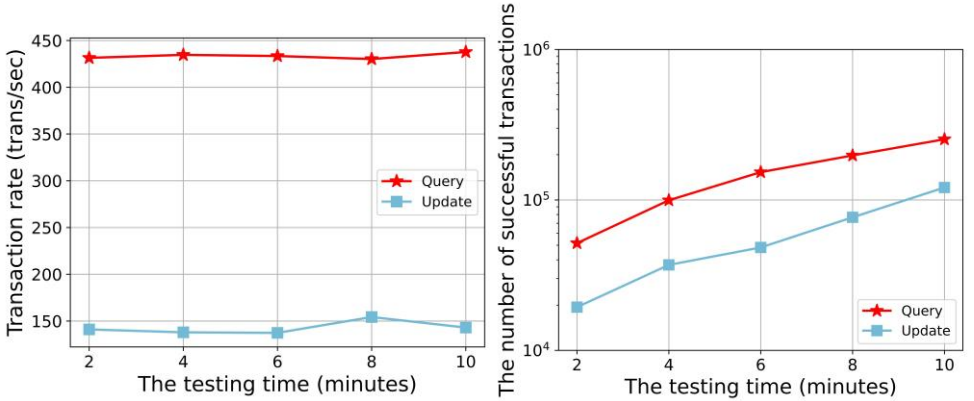
Main Contributions

- Contributions:
  - A traceable ring signature scheme utilizing the SM2 signature algorithm, facilitating traceability without the need for centralized trust;
  - A data sharing scheme that incorporates SM2-based traceable ring signature and blockchain technology;
  - Comprehensive security analysis and performance evaluation demonstrate effectiveness and efficiency.



(a) Query (b) Update

Fig. 2 The results of http_load



(a) The transaction rate (b) The successful transactions

Fig. 3 The results of siege

We employed the web testing tools http_load and siege to assess the query and update operations of our implementation with Hyperledger Fabric within a laptop enviorment. We achieved a satisfactory performance with a mean waiting time of less than 400 ms and a transaction throughput exceeding 100 per second.