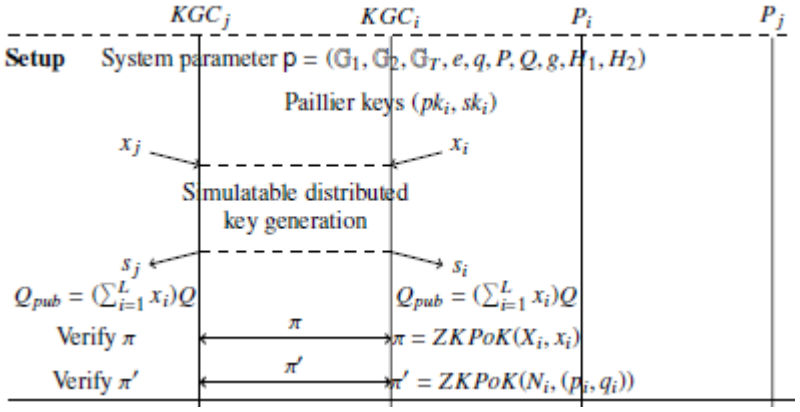
Fully Distributed Identity-Based Threshold Signatures with Identifiable Aborts

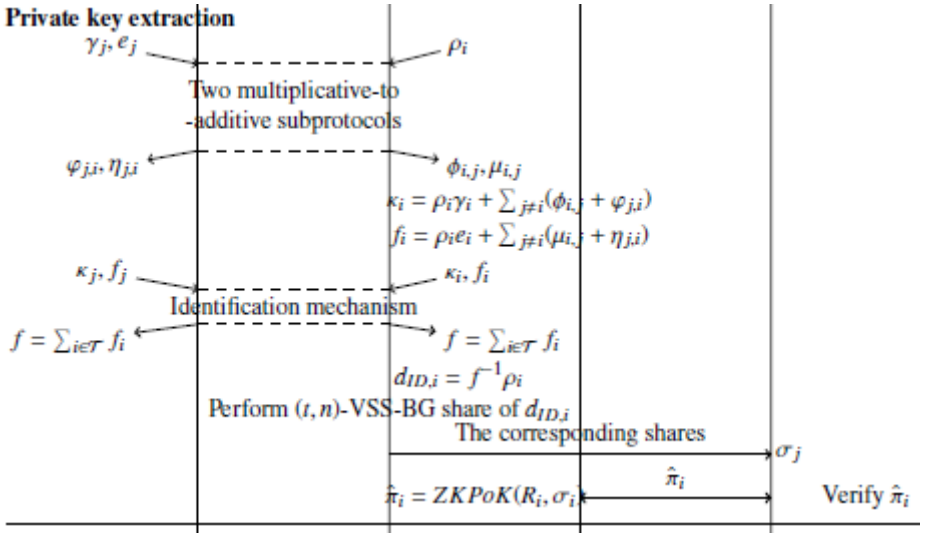
Yan JIANG, Youwen ZHU, Jian WANG, Xingxin LI

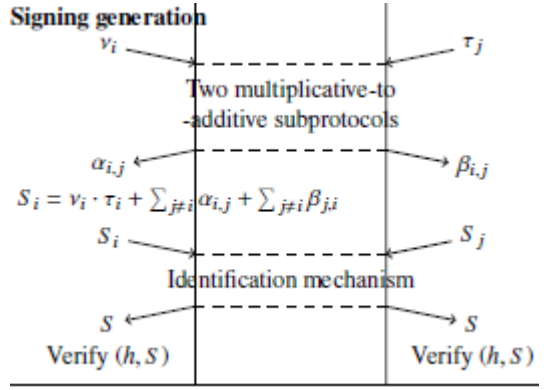
Frontiers of Computer Science, DOI: 10.1007/s11704-022-2370-4

Problems & Ideas

- Problems of fully distributed identity-based threshold signatures (IDTS):
  - Most IDTS schemes have a trusted dealer generate the private key for every party.
  - Existing IDTS solutions are vulnerable to denial-of-service attacks in the dishonest majority setting.
- Ideas: A full IDTS protocol is that it supports multiparty signatures with trustless key generation and identifiable aborts.



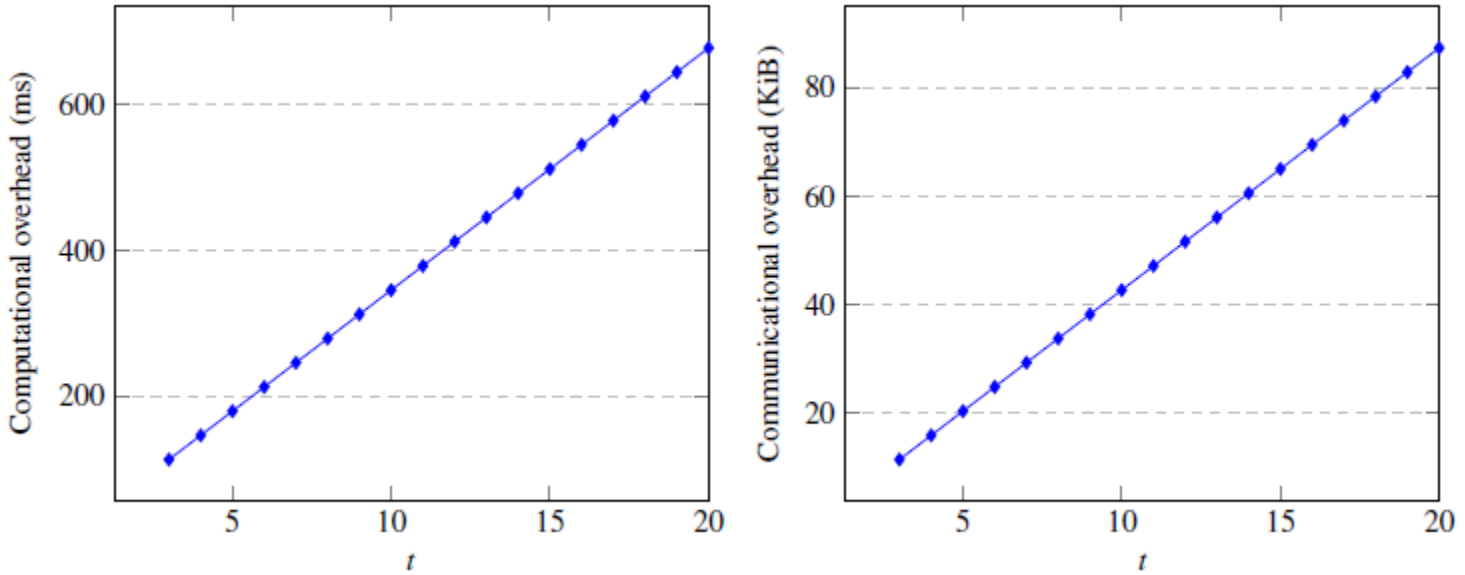




Figures demonstrate the framework of our protocol, which consists of setup, private key extraction, and signing generation. The manuscript presents fully distributed identity-based threshold signatures (IDTS) with identifiable aborts. Further, we achieve a full threshold protocol by generating both the private key and signature in a distributed manner. The paper provides security that the faithful parties kick the malicious parties out and then restart the discontinuing protocol.

Main Contributions

- Contributions:
  - Fully distributed protocol. We present a fully distributed threshold BLMQ protocol that addresses the key escrow problem. The proposed protocol does not require the trusted dealer, and generates the private key and signature both in a distributed manner.
  - Collusion Resistant. We utilize different security thresholds to construct suitable verifiable secret sharing schemes, and can resist the collusion between KGCs and signers.
  - Identifiable aborts. We design an identification mechanism which allows the honest parties to detect the identity of cheaters in case of failure.



The total costs for each signer of signing from 2 to 20 parties. Left: the computation overhead of each party; Right: the communicational cost is how much each party sends to each other party.