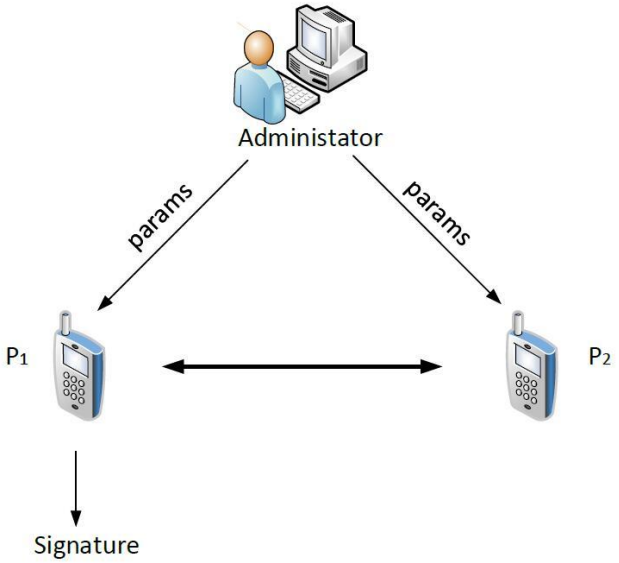
A provable-secure and practical two-party distributed signing protocol for SM2 signature algorithm

Yudi ZHANG, Debiao HE, Mingwu ZHANG, Kim-Kwang Raymond CHOO

Frontiers of Computer Science, DOI: 10.1007/s11704-018-8106-9

Problems & Ideas

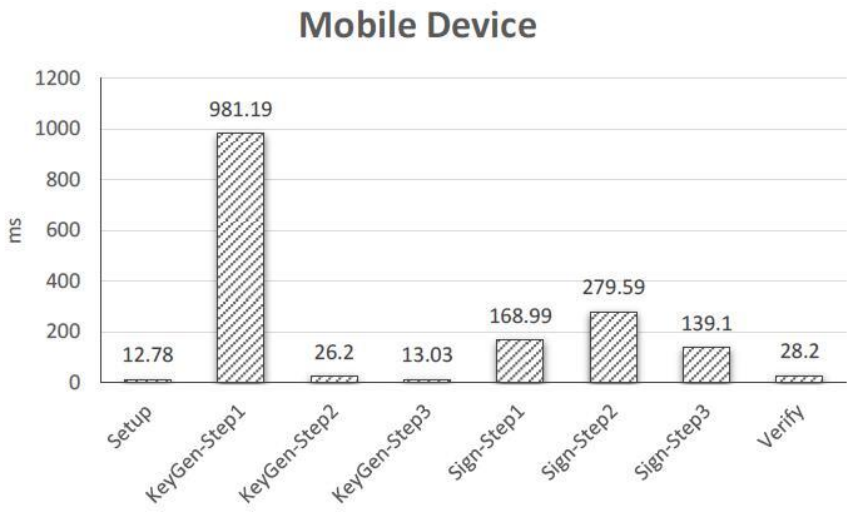
- Problems of the private key in the devices being easily leaked in wireless environment
  - Private key is usually stored on a single device which can be corrupted by an adversary.
  - The existing threshold secret sharing schemes generally suffer from key reconstruction attack.
- Ideas: Construct a two-party distributed signing protocol without reconstructing the private key
  - We proposed an efficient and secure two-party distributed signing protocol for SM2 signature algorithm.
  - The performance of the implement showes that our protocol can be deployed in practice to prevent key disclosure.



The Network Model

Main Contributions

- **Run Time on Mobile Device**



- **Run Time on PC**