Secure Systems Group, Aalto University

Application to PBFT, RePBFT and Zyzzyva

SACBFT Tranformation:
• Single active trusted counter:
  • not all replicas may have TEEs: e.g. for autonomous systems and internet-of-things applications.
  • allows gradual phase-out of TEE models over time.
• Single voting phase:
  • each request is bound to a monotonic counter value; hence the primary cannot equivocate.
  • eliminates the need for multiple voting phases.
• O(n) communication complexity:
  • most TEE-based BFT protocols are incompatible with signature aggregation, because TEE state varies between replicas.
  • a single trusted counter does not need synchronization, so all replicas always sign the same thing.

Evaluation
Test setup:
• 5 physical machines
• No faulty replicas
• 1024B transaction size
• 8Mbit/s per machine

Future work
• Adapt this approach to the PBFT view-change.
• Minimize public-key operations, e.g. through secret sharing.
• Optimize for IoT scenarios such as self-driving cars.
• Generalize the ordering primitive for use in other settings.