

1 Introduction

Concepts

Threats: faults, errors, failures.

Techniques: tolerance, prevention, removal, prediction.

Properties: reliability, availability, safety, confidentiality, integrity.

Measures: MTTF, MTTR.

Models

Components: processes (parties), network channels, message passing.

Time: synchronous, partially synchronous, asynchronous.

Channels: point-to-point, broadcast, reliable, authenticated, secret.

Failures: fail-stop, crash, omission, crash/recovery, arbitrary (Byzantine).

Formal models: I/O automata, unbounded time (distributed systems), Turing machines, polynomial time (cryptography).

Techniques

Group communication: service replication; reliable broadcast, view-synchrony, view-based group communication; consensus, impossibility of asynchronous consensus; failure detectors, consensus, atomic broadcast.

Distributed cryptography: secret sharing; threshold cryptography, threshold encryption, threshold signatures, and threshold pseudorandomness; proactive security.

Service replication: state machines, atomic broadcast protocols.

Data replication: quorums, distributed storage, erasure coding.

Applications

- Cluster computing
- Secure distributed services (e.g., DNS)
- Networked storage (Cryptographic file systems)

Literature for the course

- [AW04] H. Attiya and J. Welch, *Distributed computing: Fundamentals, simulations and advanced topics*, second ed., Wiley, 2004.
- [CDK01] G. Coulouris, J. Dollimore, and T. Kindberg, *Distributed systems: Concepts and design*, 3rd ed., Addison-Wesley, 2001.
- [GR06] R. Guerraoui and L. Rodrigues, *Introduction to reliable distributed programming*, Springer, 2006.