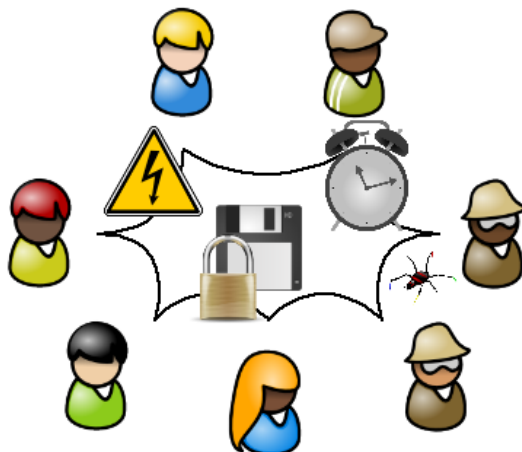


1 Introduction



1.1 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, non-determinism, unbounded time (for distributed systems), Turing machines, polynomially-bounded time (for cryptography).

1.2 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.

1.3 Applications

Cluster computing: Reliable services in Java.

Distributed services: Security in the domain-name system (DNS), highly available storage for large-scale service providers.

Networked storage: Secure storage systems, distributed file systems.

1.4 Literature

There is no single book that contains all material of the course. The following books have a large overlap with the material on crash-tolerant protocols: Two of them [AW04, GR06] focus on algorithms and models; the other one [CDK05] is more oriented toward applications and presents some example systems in detail, and also touches on the basics of cryptography.

[AW04] H. Attiya and J. Welch, *Distributed computing: Fundamentals, simulations and advanced topics*, second ed., Wiley, 2004.

[CDK05] G. Coulouris, J. Dollimore, and T. Kindberg, *Distributed systems: Concepts and design*, 4th ed., Addison-Wesley, 2005.

[GR06] R. Guerraoui and L. Rodrigues, *Introduction to reliable distributed programming*, Springer, 2006.

Specific literature references will be included in the lecture notes and will be posted on the course web page:

<http://www.zurich.ibm.com/~cca/sft09/>