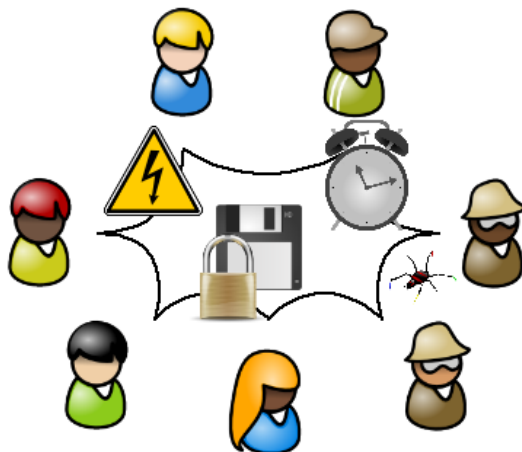


## 1 Introduction



### 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).

**Networked storage:** Secure storage systems, cryptographic file systems.

## **Books 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.

More literature references are available on the course web page:

<http://www.zurich.ibm.com/~cca/sft08/>