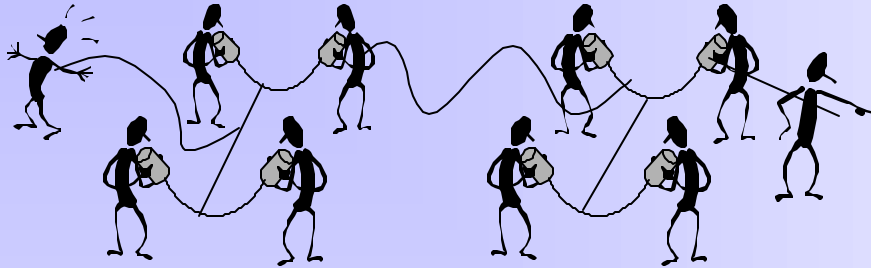


CLIQUEES: security services for dynamic peer groups



Decentralized authenticated group key agreement with provable security



Secure and efficient group membership changes

New Ideas

- Efficient and provably secure authenticated group key agreement techniques. New security services, e.g., group integrity.
- Contributory cryptographic protocols geared towards dynamic peer groups irrespective of underlying communication paradigm, protocol layer and network topology.
- Understanding of the interplay and inter-dependence between group security protocols and reliable group communication semantics. Notably, development of techniques for efficient handling of the impact of network faults on group security protocols.

Impact

- λ Versatile and flexible CLIQUES toolkit and API offering security services for dynamic peer groups.
- λ Security services for replicated server groups, groupwork applications, multi-user games and simulations.
- λ Understanding of security requirements in dynamic peer groups, corresponding mechanisms and efficiency/performance metrics.

Schedule

