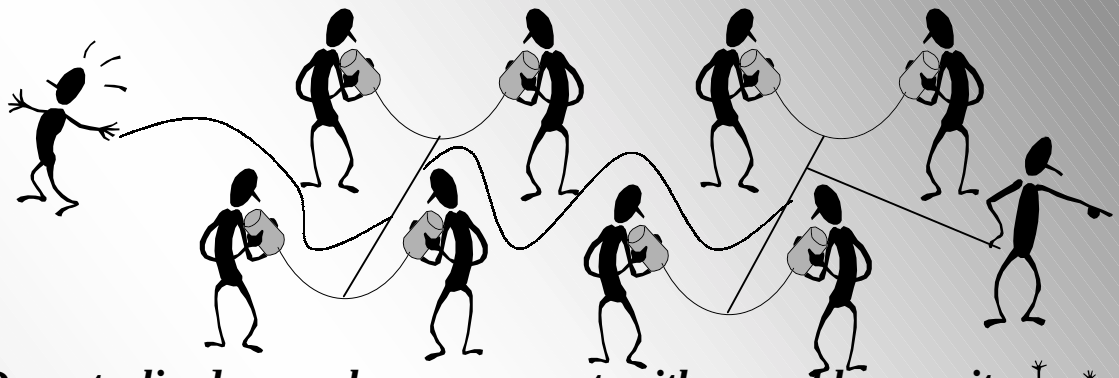
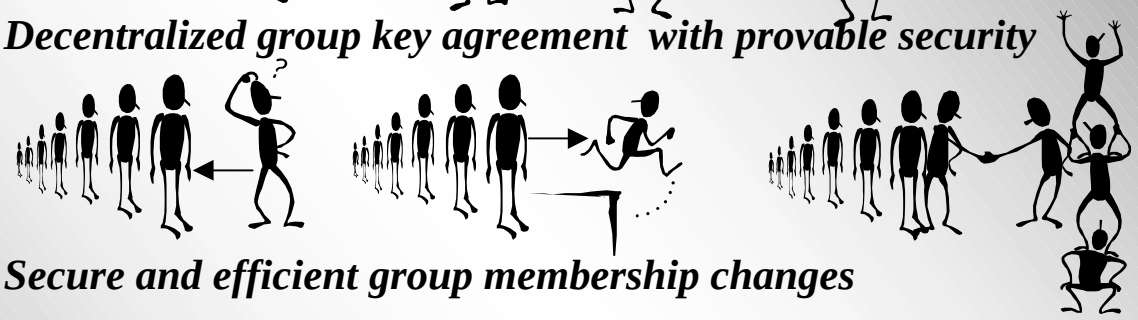
CLIQUES:

layer- and network-independent security services for dynamic groups



Decentralized group key agreement with provable security



Secure and efficient group membership changes

Group operations:
- Initial key agreement & re-key
- Member deletion & addition
- Mass join & leave
- Group fission & fusion

Key agreement services:
- Implicit key authentication
- Key confirmation
- Key integrity
- Non-repudiation of membership

Group Security Services:
- Authentication to outsiders
- Intra-group authentication
- Group signatures
- Anonymity
- Encryption for and within group

Anticipated applications:
- Voice- and video-conferencing
- Large-scale metacomputing
- Routing and other global network services
- Restricted email groups

Current activities:

- *CLIQUES API under development (JAVA/Solaris)*
- *Definition of non-repudiation services*
- *Investigation of scalability issues*

Publications:

- *CLIQUES: a new approach to group key agreement, IEEE ICDCS'98*
- *Secure Group Barter, Financial Crypto'98*
- *A Protocol Suite for Group Key Management, (ISI TR) in submission*
- *Authenticated Group Key Agreement, in submission*

Contact info:

- *http://www.isi.edu/div7/CLIQUES, email: gts@isi.edu*

Project Staff: G. Tsudik, G. Ateniese **Collaborators**: IBM Research **Duration:** 07/97-06/00