CLIQUES: Secure Services for Group Communication

Gene Tsudik
gts@isi.edu

DARPA High Confidence Networking Workshop, 06/12/98, Rockport, MA.

The Setting

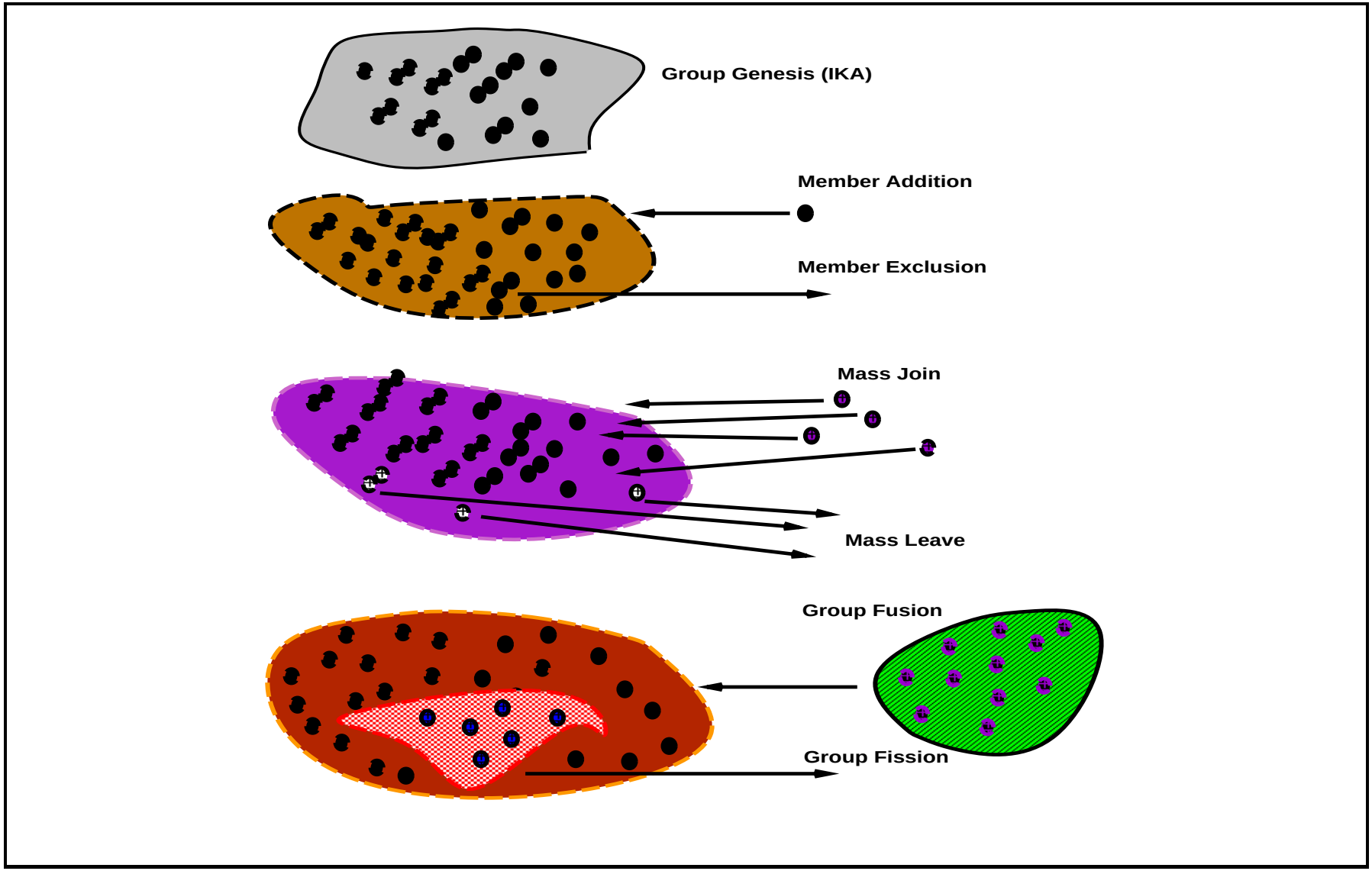
Dynamic Peer Groups (DPGs):

- Relatively small (100s of members)
- No Hierarchy
- Frequent Membership Changes
- Elected or Appointed (but not permanent) Group Controller

Notable Examples:

- Replicated Servers
- Group-work
- Video/audio Conferencing
- Ad Hoc Networks

DPG Membership Operations



The Problem

How to maintain security with constantly changing membership?

Security Services in DPG setting:

- Authentic, private communication within group
- Authentic, private communication with outsiders
- Authentication flavors: *any* member or *specific* member
- Group signatures
- Non-repudiation of Membership

Observations:

- Centralized (TTP) approaches do not work well
- Simple extensions of 2-party methods are inefficient
- Key Agreement – most basic service
- **NOTE:** Key Distribution $\neq$ Key Agreement

Variables

Key Agreement:

- IKA: Initial Key Agreement (group genesis, re-key)
- AKA: Auxiliary Key Agreement (membership changes)
- Centralized: Key Distribution/Transport
- Contributory: Equal Share by Everyone

Design Parameters:

- Diffie-Hellman model
- Contributory KA
- Group Controller (fixed or floating)
- No **a priori** ordering
- No policy assumptions!
- No reliance on local environment

Progress...

Publications:

- *"Diffie-Hellman Key Distribution Extended to Groups"*, 1996 ACM CCCS.
- *"CLIQUES: A New Approach to Group Key Agreement"*, 1998 IEEE ICDCS.
- *"Authenticated Group Key Agreement and Friends"*, 1998 ACM CCCS.
- *"Key Agreement in Dynamic Peer Groups"*, in submission.
- *"An Efficient Group Signature Method"*, in submission.
- *"Group Barter: Multi-Party Fair Exchange..."* 1998 Financial Cryptography.

Real Work:

- CLIQUES Toolkit: JAVA, C/C++ (under dev.)
- Collaboration with JHU (SPREADS, COMMEDIA)
- Collaboration with IBM Research (RS6K, etc.)
- ISI's GLOBUS Metacomputing project

Eagerly looking for other collaboration opportunities!!!

Membership Changes

Protocols:

- Member Addition
- Member Deletion
- Mass Join *
- Mass Leave *
- Group Fusion

Properties:

- **Key Independence**
- Security equivalent to IKA (poly. ind.)
- Fixed/Floating Controller
- Anyone can be group controller (subject to policy)
- Group controller can be easily excluded

Authenticated Key Agreement

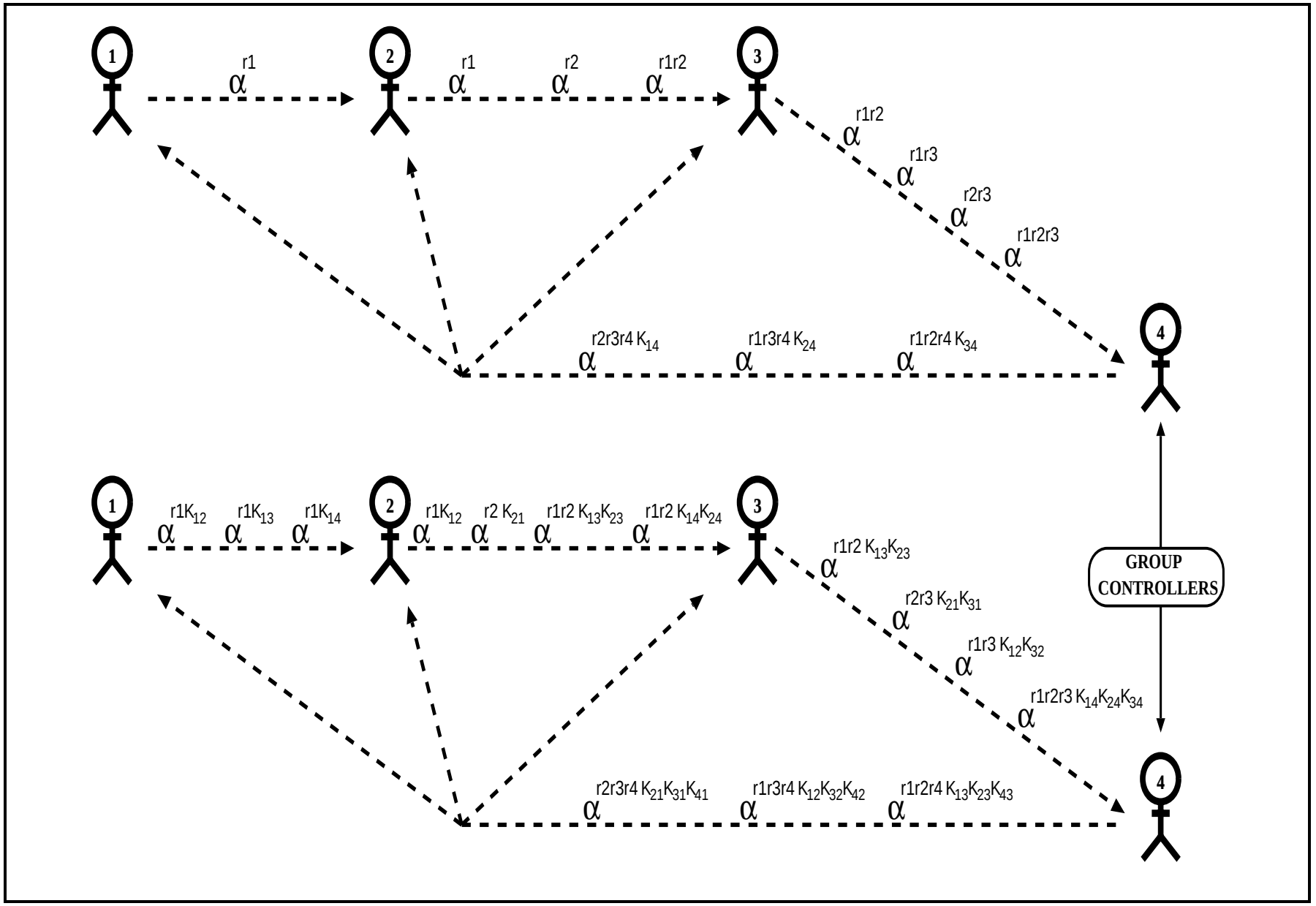
Protocols:

- A-DH: 2-party, 2-round, PFS, KKA-resistant
- A-GDH.2: n-party, n-round, A-DH/GDH.2 blend
  $M_n \longrightarrow M_i$ auth.
- SA-GDH.2: n-party, n-round
  $M_i \leftrightarrow M_j$ auth.

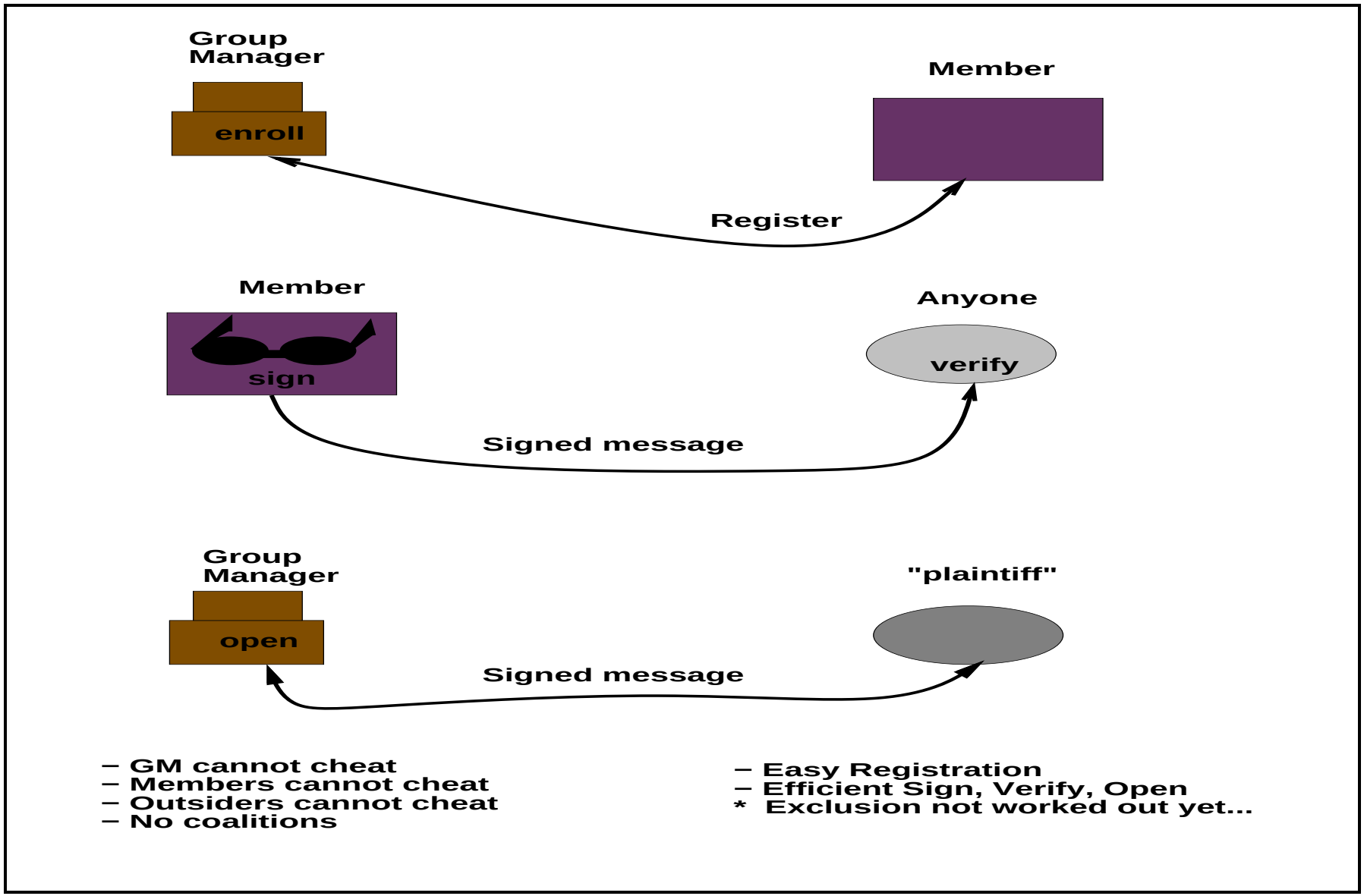
Properties:

- Inherited: Key Independence, Passive Attack Resistance
- PFS
- KKA Resistance
- Key Confirmation
- Key Integrity (???)
- Group Integrity
- (Partial) Entity Authentication

Authenticated Key Agreement



Group Signatures



- GM cannot cheat
- Members cannot cheat
- Outsiders cannot cheat
- No coalitions

- Easy Registration
- Efficient Sign, Verify, Open
- * Exclusion not worked out yet...

On-going and Future Work

- Member (entity) authentication
- Encryption for/within group
- Authentication of specific and anonymous group members
- CLIQUES Toolkit available 1998
- API definition, performance measurements, integration experience
- Group Signatures

CLIQUES HOME PAGE: www.isi.edu//div7//cliques