# Collaborative Security

Gene Tsudik

Computer Networks Division, USC/ISI
*gts@ics.uci.edu*
*http://www.ics.uci.edu/~gts*

and

Information and Computer Science Department, UC Irvine
*gts@isi.edu*
*http://www.isi.edu/~gts*

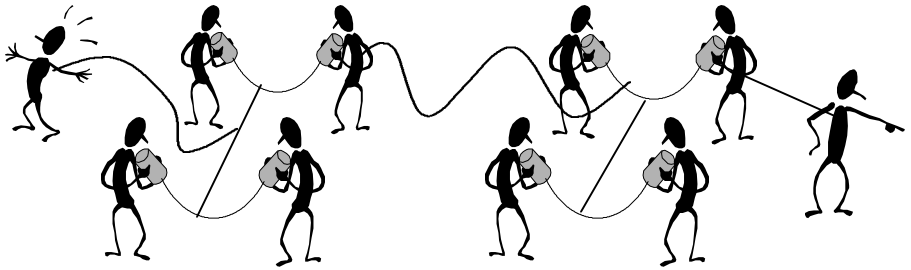
# Group Communication

- One-to-many
  - Single-source broadcast: cable/sat. TV, radio, etc.
- Few-to-many
  - Multi-source broadcast (2-tiered groups): televised debates, GPS, time, etc.
- Any-to-any
  - Collaborative applications: conferencing, mailing lists, visualization, instrument control, simulations, replicated servers, etc.

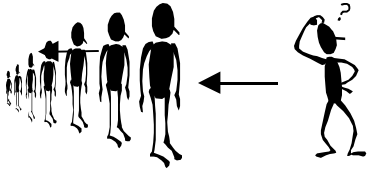
  Rich communication semantics, tighter control, more emphasis on **security**

# *CLIQUES:* Security in Dynamic Peer Groups

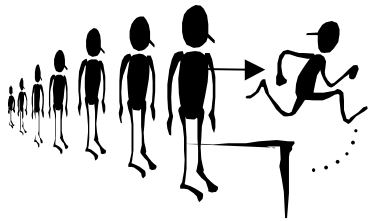
(DARPA/ITO HCN, 07/97-06/00)



Formation



Member add



Member leave

Group merge

Group partition

# Background

Targeted environment

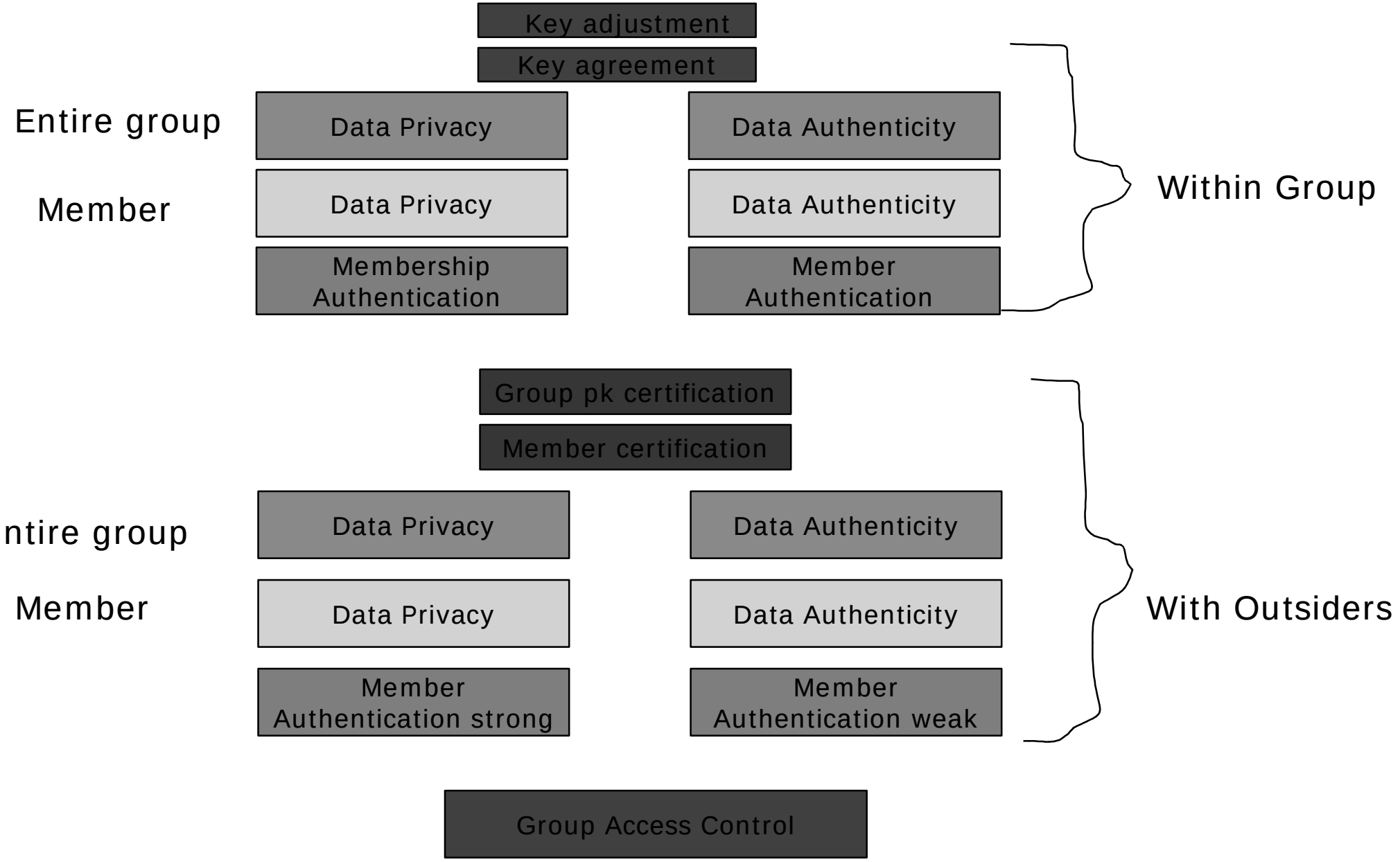
- Relatively small groups
- Dynamic membership
- No hierarchy
- Any-to-Any
- Collaborative applications

Problem:

how to obtain security in peer groups with dynamic membership and decentralized control?

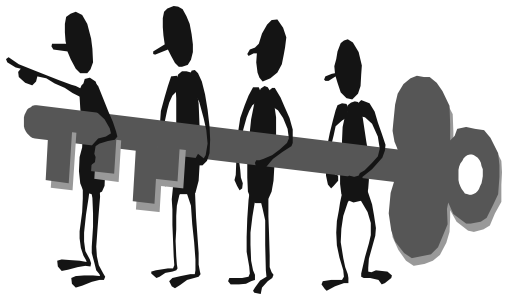
Complexity >> 2- and 3-party security

# Security Services



# Group Diffie-Hellman

## Important features:



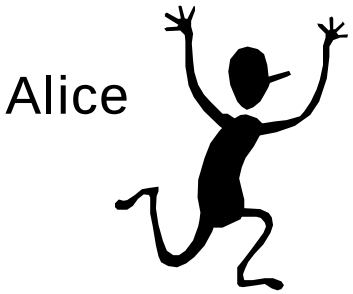
- **Formal** proof of security
- Decentralized.
- No ordering, no synchronization (sort of)
- No topology or network dependencies
- Group controller: floating or fixed (chore, not privilege!)
- Everyone contributes to the key.
- Everyone can prove they took part in the generation of the key.
- Two message latency for join of 1 member
- One message latency for leave of N members.
- N+1 message latency for join/merge of N members

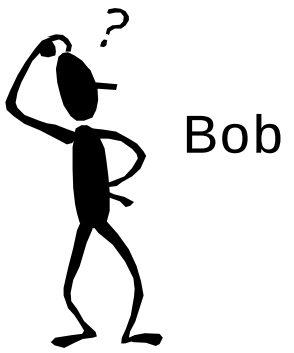
## Why key agreement?

- Centralized (TTP) approach: single-point, too much load
- 2-,3-party extensions unscalable: n*n message exchanges

# Diffie-Hellman Primer (DH78)

$p$ – large prime (≥ 512 bits)
$Z_p^* = \{1,..., p-1\}$
$g$ – base (generator)




$a \in_R Z_p^*$

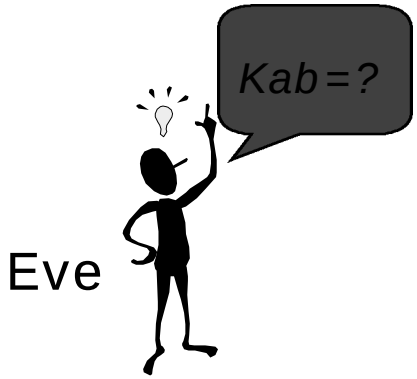
$A = g^a \bmod p$

$b \in_R Z_p^*$

$B = g^b \bmod p$

$K_{ba} = A^b \bmod p$

$K_{ab} = B^a \bmod p$



# DH Primer (contd)

Discrete Log Problem :

*Given* : $A = g^a \bmod p$

*FIND* : $a$

Diffie – Hellman Problem :

*Given* : $A = g^a \bmod p$ *and* $B = g^b \bmod p$

*FIND* : $g^{ab} \bmod p$

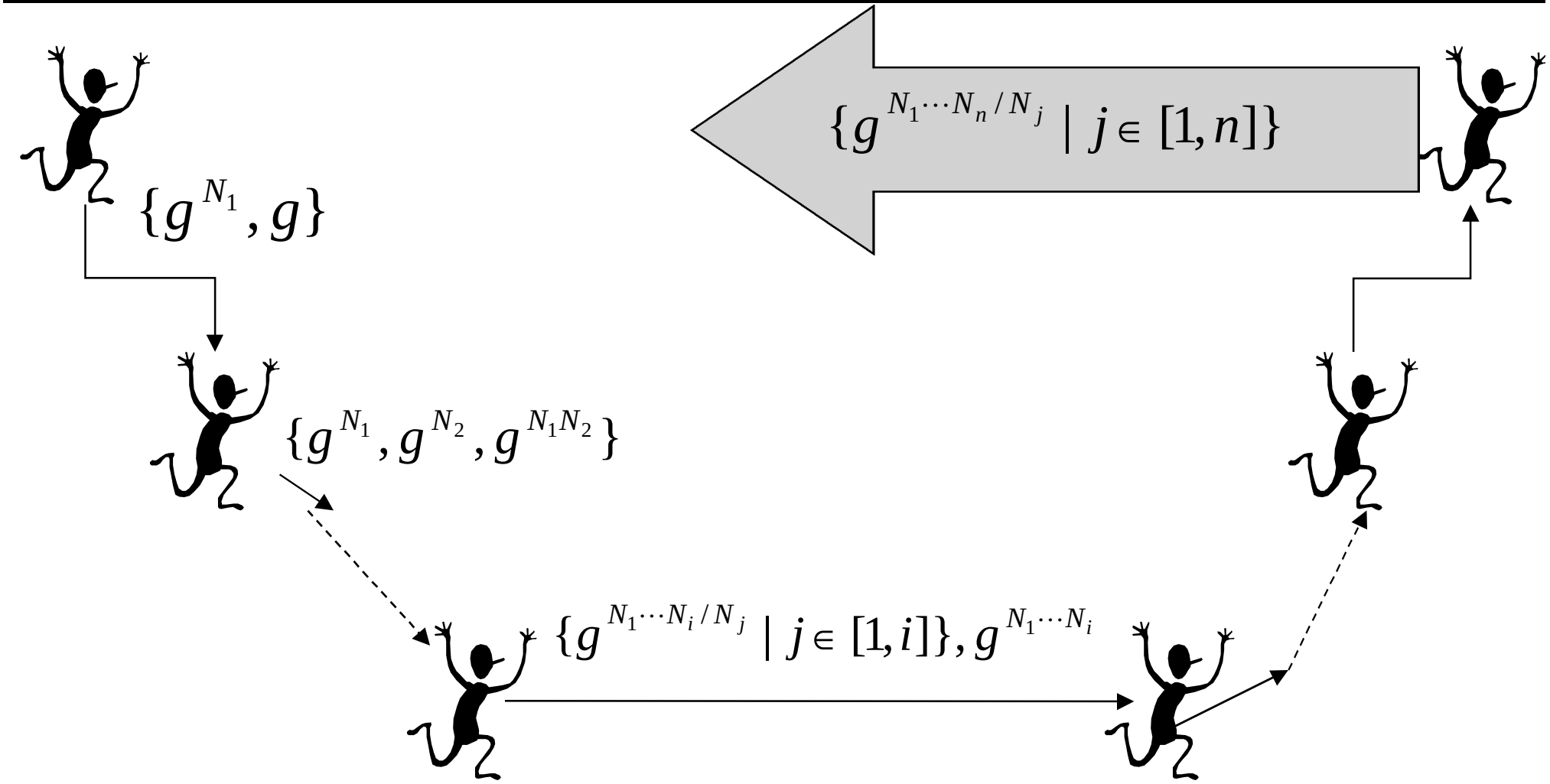
Decision DH Problem :

*Given* : $A = g^a \bmod p$, $B = g^b \bmod p$

*Distinguish* : $K_{ab} = g^{ab} \bmod p$

*from a random number!*

# GDH Key Agreement



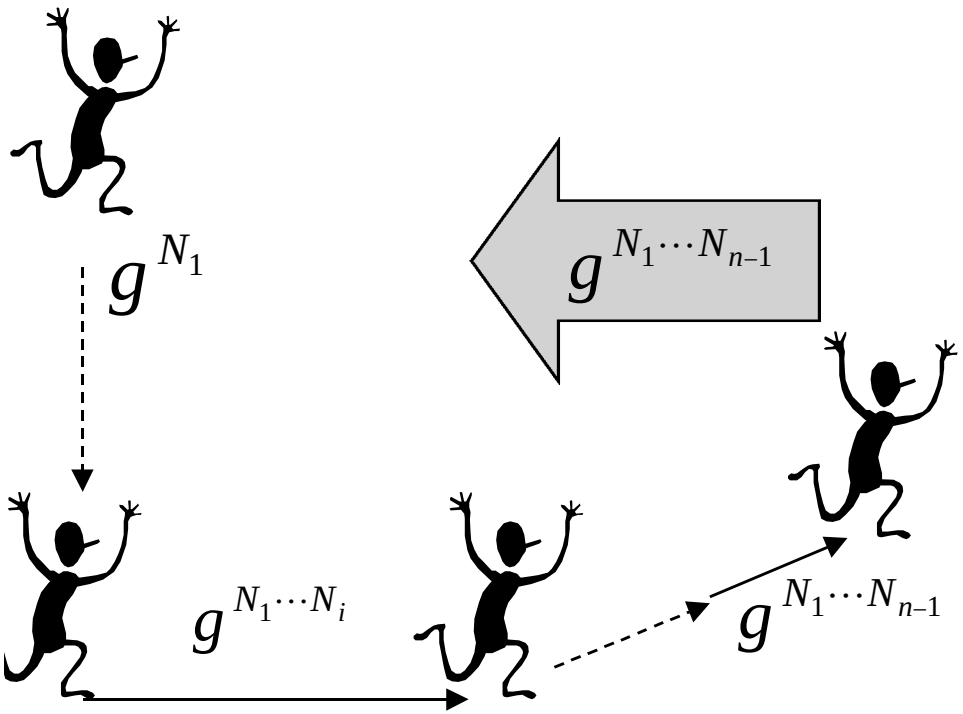

$_n = g^{N_1 \cdots N_n} \bmod p$

olynomially indistinguishable
om random number!

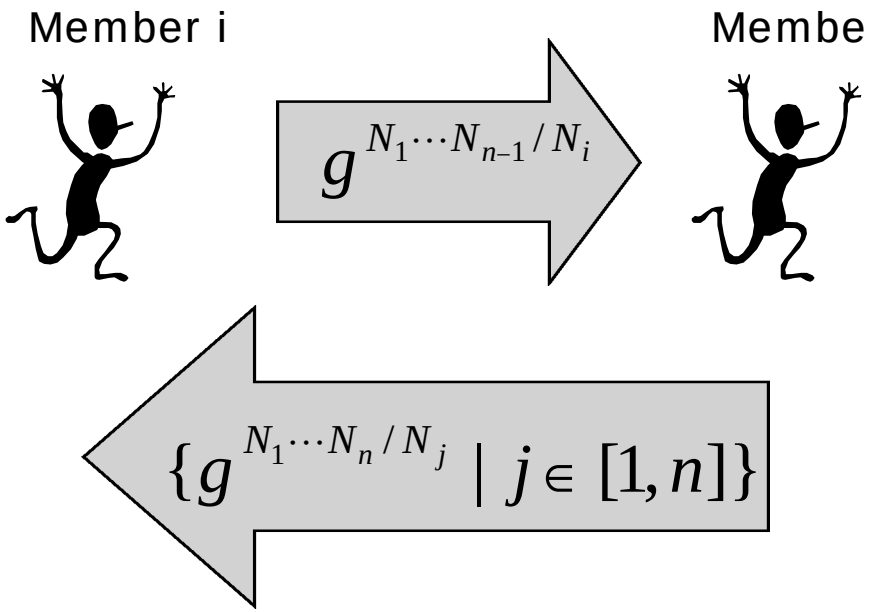
Key adjustments/refresh protocols
easily derived and shown secure

# Another GDH Key Agreement

Stage 1



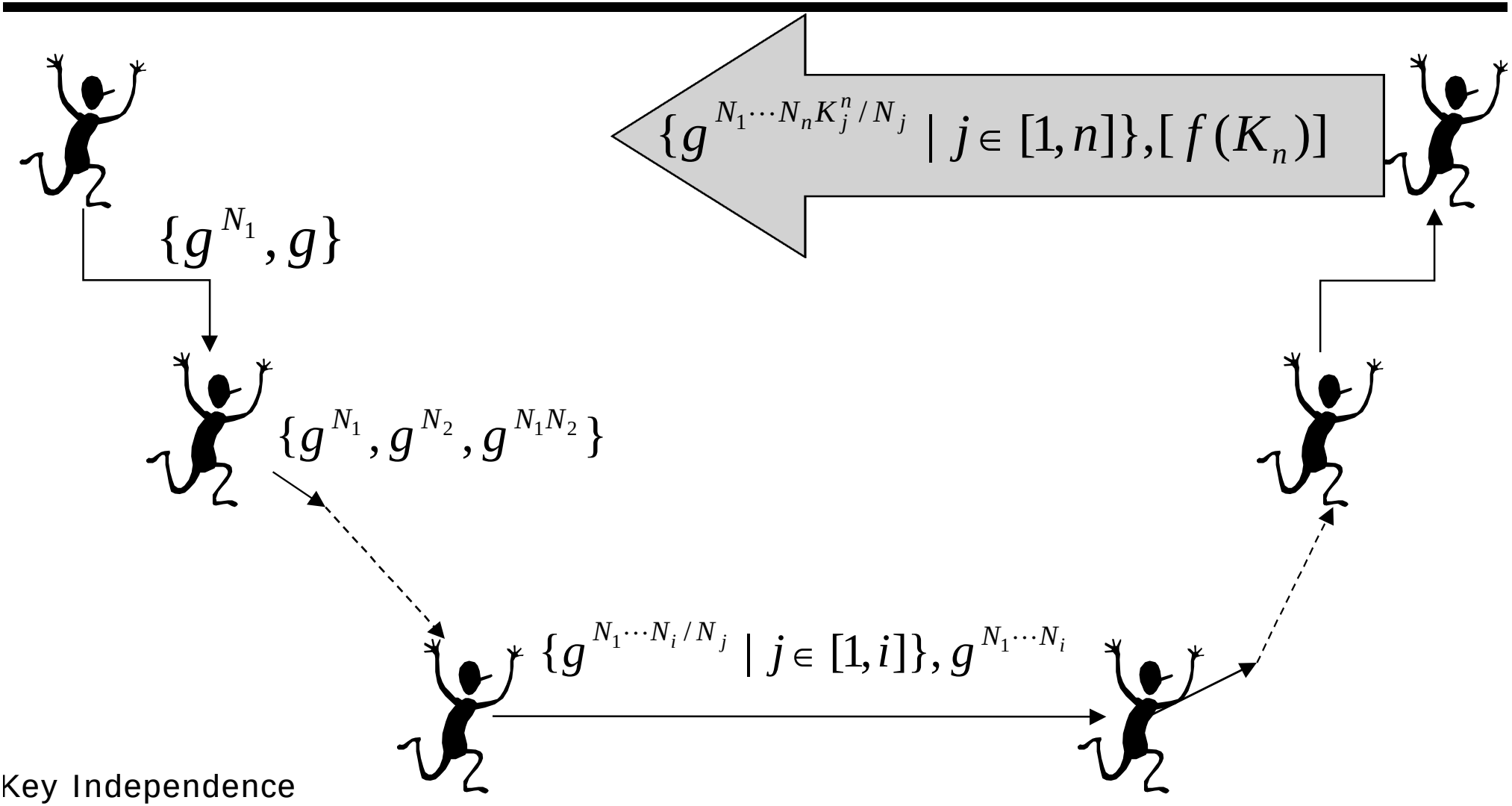

Stage 2




$$K_n = g^{N_1 \cdots N_n} \bmod p$$

- 2 exponentiations per member
- lots of communication

# Authenticated GDH Key Agreement

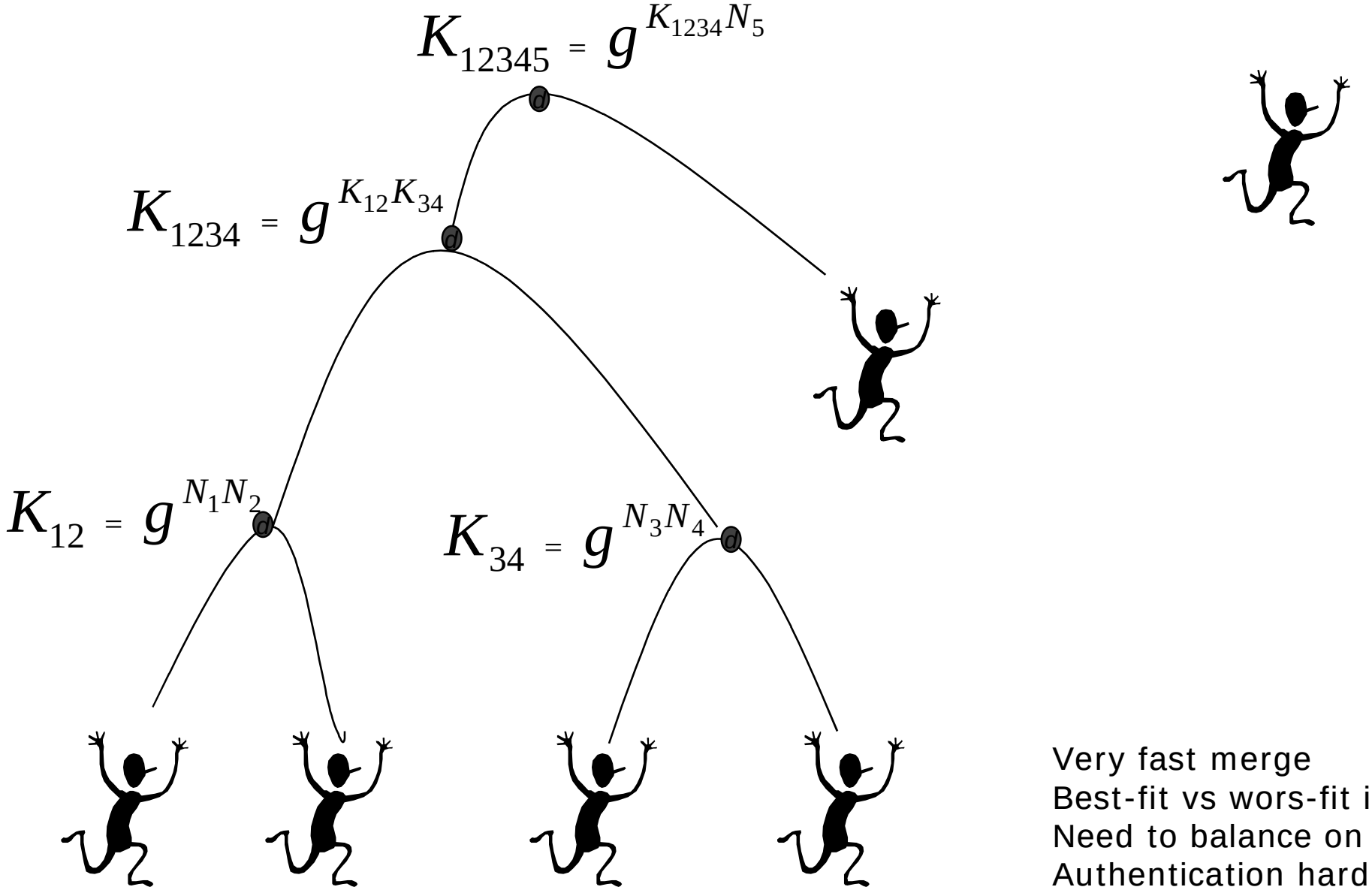



Key Independence
Perfect Forward Secrecy
KKA Resistance
Key Confirmation
Key Authentication

Stronger version:
- Membership Integrity
- Partial entity authentication

$$K_{ij} = g^{S_i S_j} \bmod p$$

# OFT-based Key Agreement



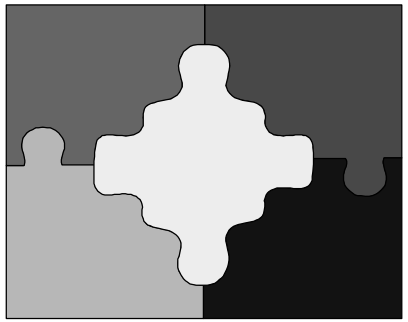

Very fast merge
Best-fit vs wors-fit inser
Need to balance on leav
Authentication hard

# Security Services Provided

- Decentralized authenticated group key agreement with provable security based on group Diffie-Helman: each member contributes equally to group key
- Membership changes: single member, many members and sub-groups
- Membership authentication and non-repudiation: based on knowledge of key-share
- Authenticated join/leave: requires long-term DH credentials

## Other pieces of the puzzle

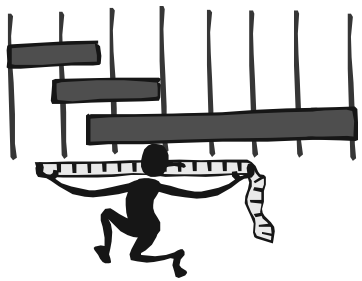
- Certification infrastructure
- Reliable group communication subsystem
- Membership Authorization / Access control



# STATUS

Protocols

- Initial Key Agreement
- Auxiliary Key Agreement (membership changes)
- Authenticated Key Agreement



Shared-key and signature strains

CLIQUES API, C implementation (rel. 1.7a)

OpenSSL as crypto base

Testing and integration with JHU's SPREAD and UCSB's TOTEI

Current performance results: O(n) exponentiations

- 12msec on SPARC ULTRA II, 2msec on PENTIUM II 450Mhz !!!

On-going integration with AKENTI Access Control Server

# CLIQUES API (contd)

Underlying group communication subsystem must provide reliable synchronized event notification for:

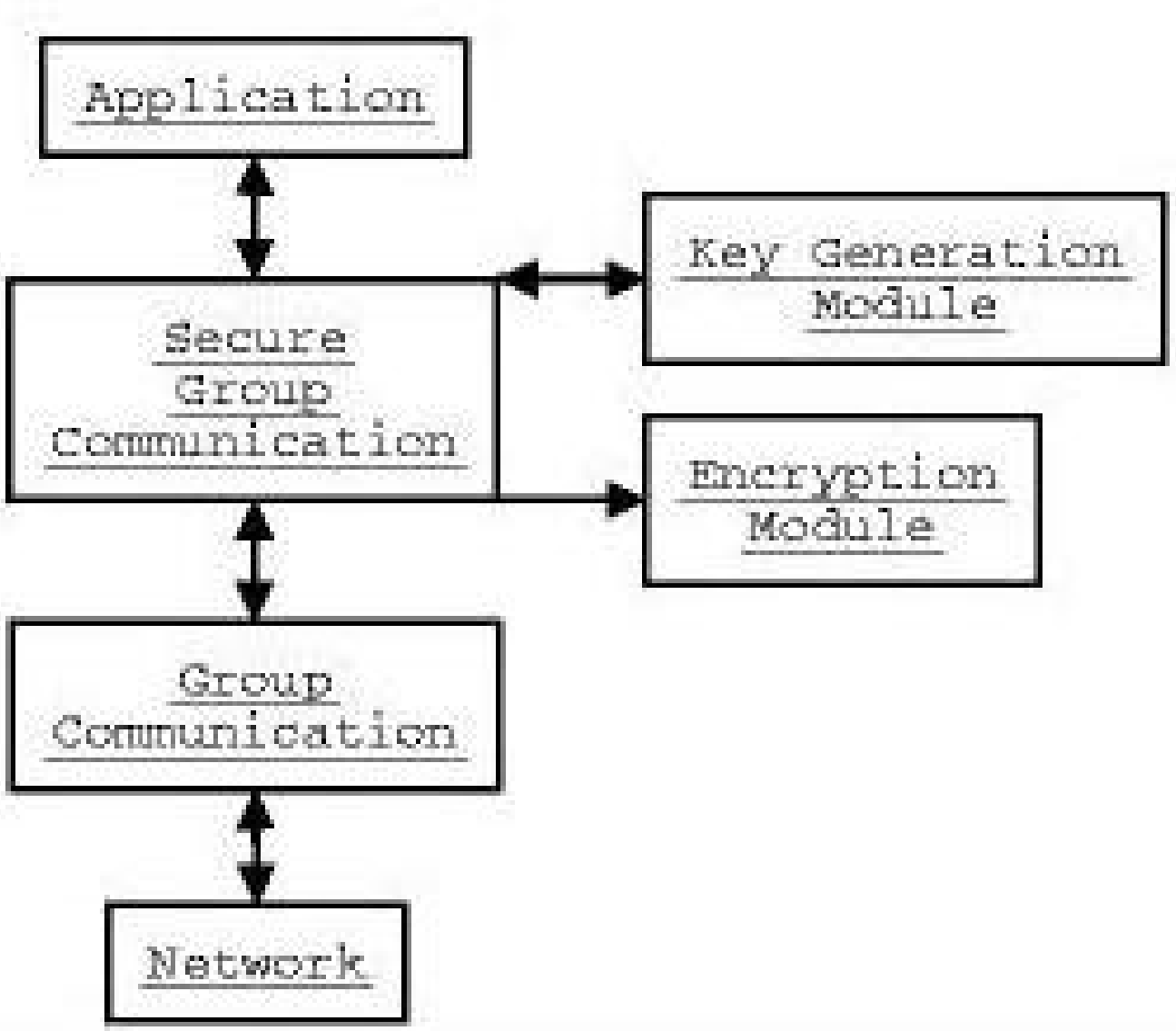
- group joins
- group leaves
- partitions
- node failures or disconnects
- merges (partition heals)


Supports primitives for:

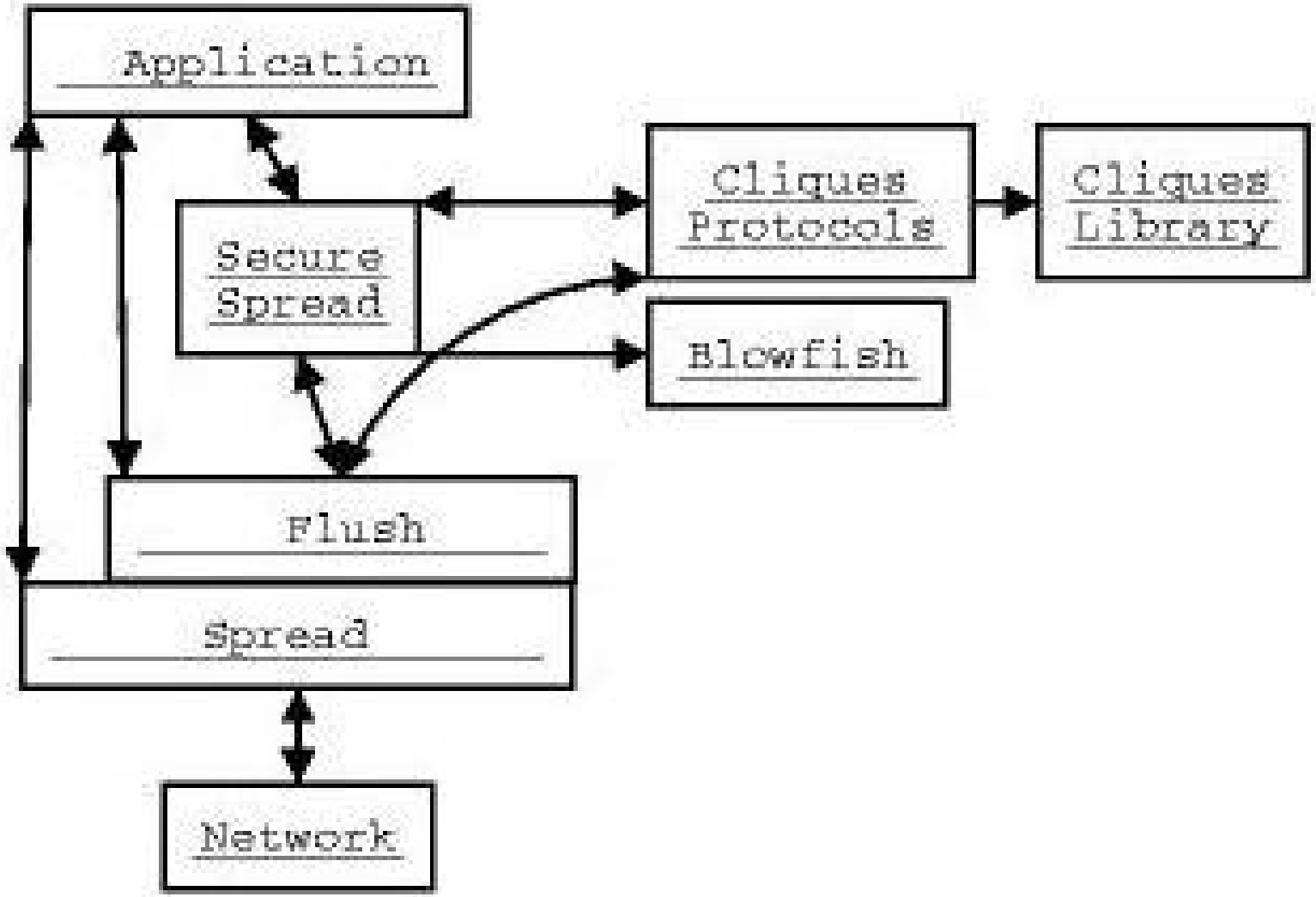
- leaves
- joins
- merges
- refreshes

Centralized and GDH key agreement (others tba)

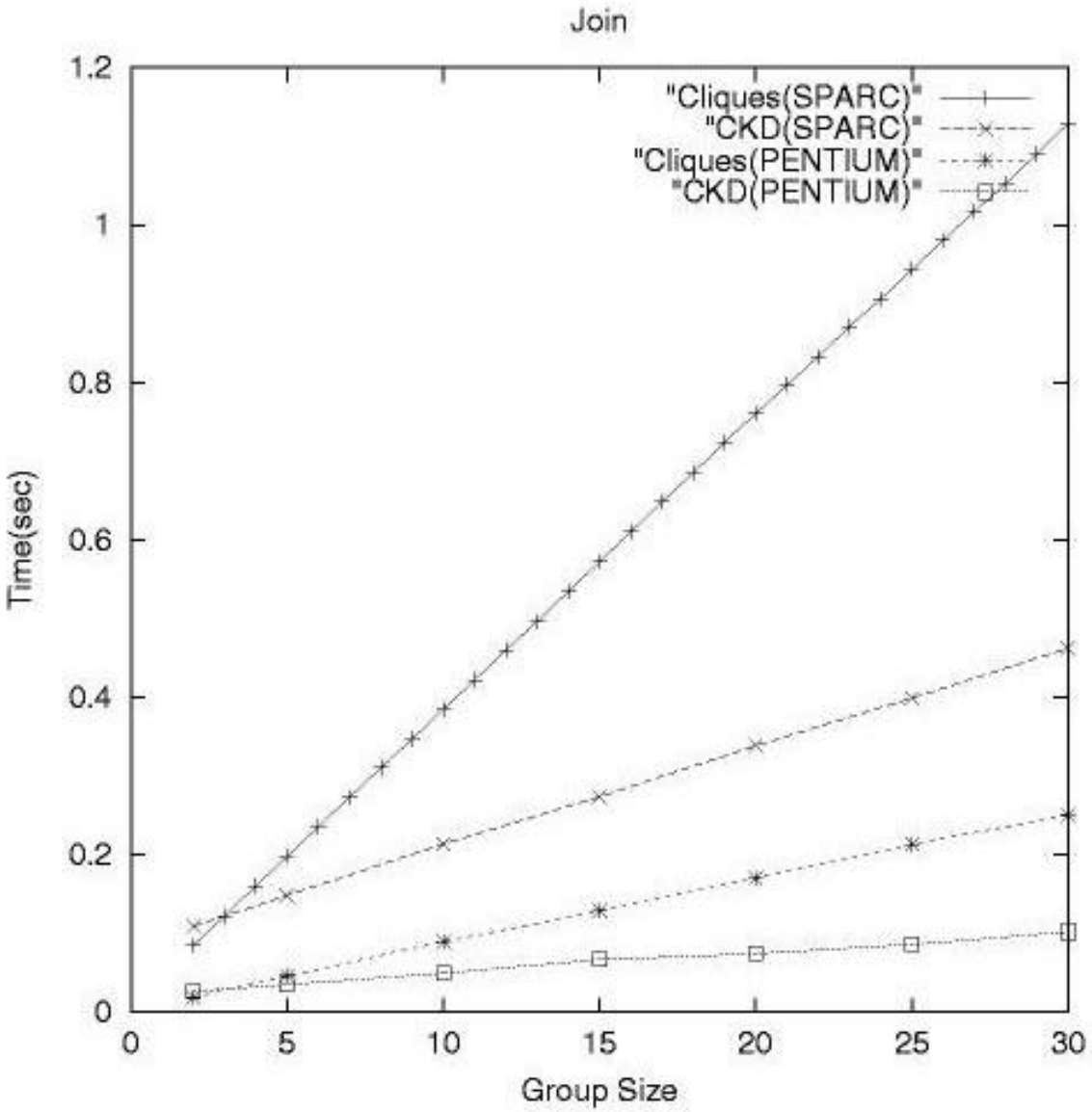
# Generic Architecture



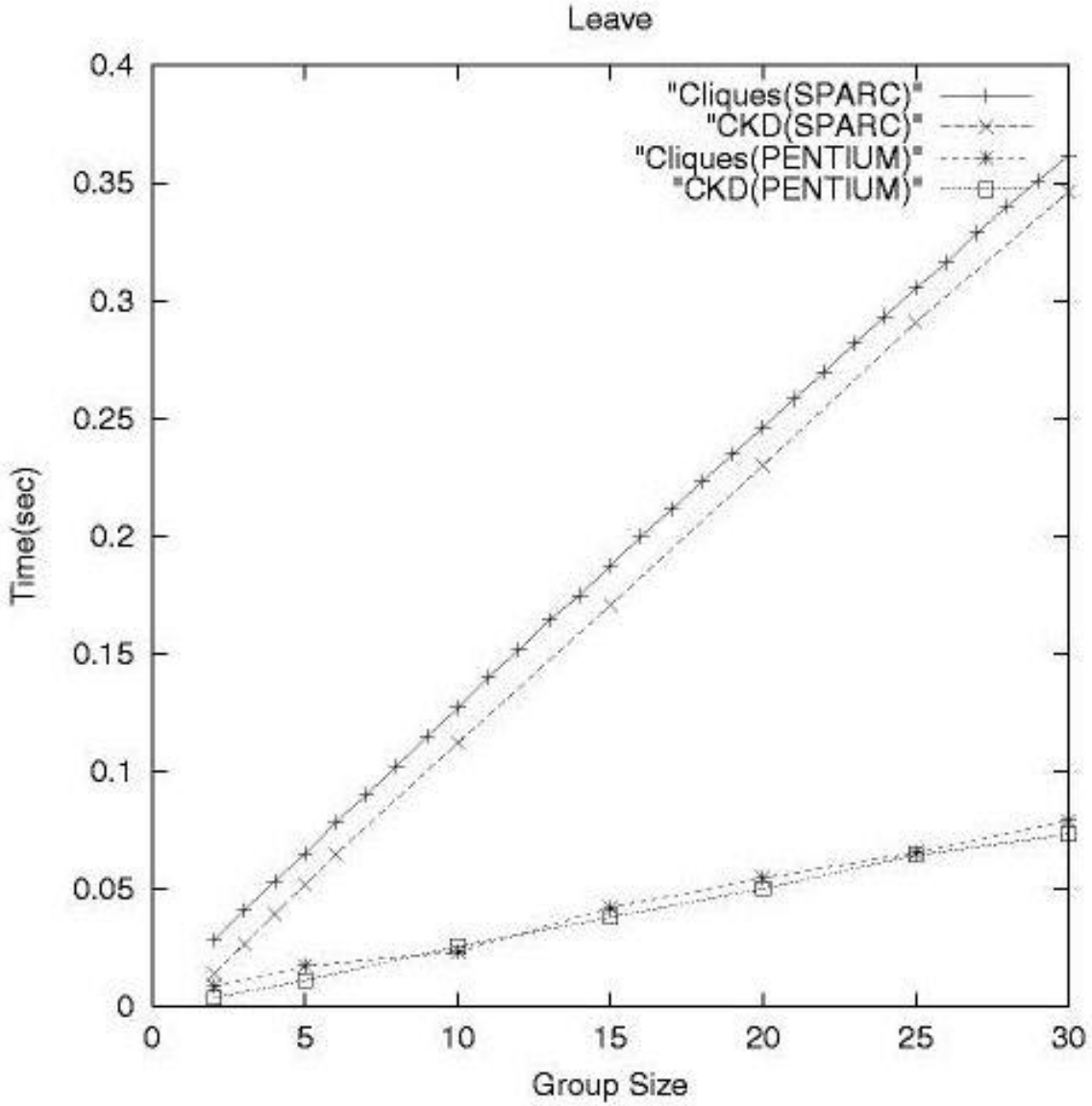
# Secure SPREAD Architecture



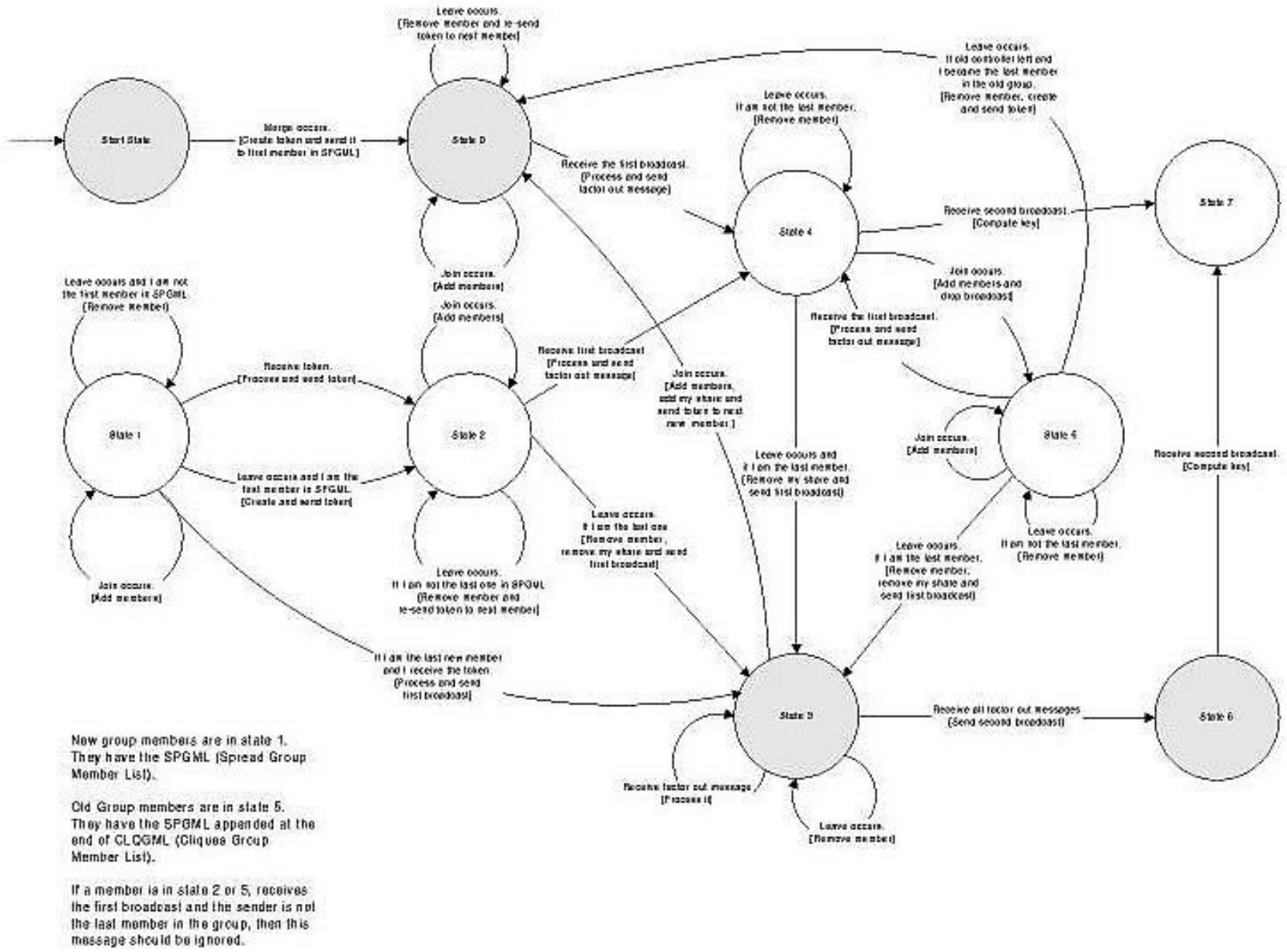
# Secure Spread: join



# Secure Spread: leave/partition



# Secure Spread: cascaded events



# Lessons learned

- Paper protocols <> real protocols
- Incremental formation of groups
- Security, group comm not a simple composition
- Comm latency vs computation (group topology!)
- Difficulty of handling many merging sub-groups
- Group size limits (100?)
  - other DH-like keys
  - elliptic curve duals
- Provable security matters!

# Challenges and directions

- Two-tiered groups (few-to-many)
- Group membership policy (Auth + AC)
  - How to specify?
  - Enforce?
- Group certification: group key, membership, etc.
  - Dynamic membership?
  - Individual vs. opaque certificates?
- How to tolerate Byzantine behavior by member(s)?
  - Cannot prevent key release or denial-of-service...
  - Member proves correct protocol execution
- Group Barter
- Group Signatures

# Related Work

Strong Group Semantics:

- Cornell: Birman et al. (ISIS, Horus, Ensemble)
- UCSB: Melliar-Smith et al. (Totem)
- HUJ: Dolev et al. (Transis)
- JHU: Amir et al. (Spread)

IP Multicast:

- TIS: Balenson et al. (OFT)
- UTA: Lam, Gouda
- NSA Wallner et al. (LKH)
- IBM: Canetti et al.
- ETHZ: Carroni, Sun (Versa)

Theory:

- Ingemarsson, Tang, Wong (ToIT 81)
- Burmester/Desmedt 94 (Eurocrypt 94)
- Steer/Diffie (Crypto'89)
- DeSantis/Vaccaro/Yung

# Publications


•M. Steiner, G. Tsudik and M. Waidner
Diffie-Hellman Key Distribution Extended to Groups, ACM CCCS'96

•M. Steiner, G. Tsudik and M. Waidner,
CLIQUES: A New Approach to Group Key Agreement, IEEE ICDCS'98

•G. Ateniese, M. Steiner and G. Tsudik
Authenticated Group Key Agreement and Friends, ACM CCCS'98

•M. Steiner, G. Tsudik and M. Waidner
Key Agreement in Dynamic Peer Groups, IEEE TPDS, submitted.

•G. Ateniese, M. Steiner and G. Tsudik
Authenticated Group Key Agreement and Friends, IEEE JSAC, April 2000.

•Y. Amir, G. Ateniese, D. Hasse, Y. Kim, C. Rotaru, J. Stanton, J. Schultz, and G. Tsudik, Spread/CLIQUES Integration Experience, IEEE ICDCS'00

• D. Hasse, Y. Kim, O. Chevassut and G. Tsudik,
The Design of Group Key Agreement API, DARPA DISCEX'00.

# Summary

Impact:
- IBM
- JHU
- LBNL
- IRTF

CLIQUES web page: http://www.isi.edu/div7/cliques
- API documentation
- Publications
- Presentations

API code by request from gts@isi.edu

Collaborators:
- IBM Research, Johns Hopkins, LBNL, Nortel

People:
- G. Ateniese, O. Chevassut, D. Hasse, Y. Kim, G. Tsudik

# Other current research

- Integrated and Reliable Multicast in Ad Hoc Networks (NSF)
- Secure IP multicast (Nortel)
- Survivability Using Controlled Security Services (DARPA)
- Server-Assisted Digital Signatures (NSA)
- Access Control in Collaborative Applications (DoE, w/LBNL)