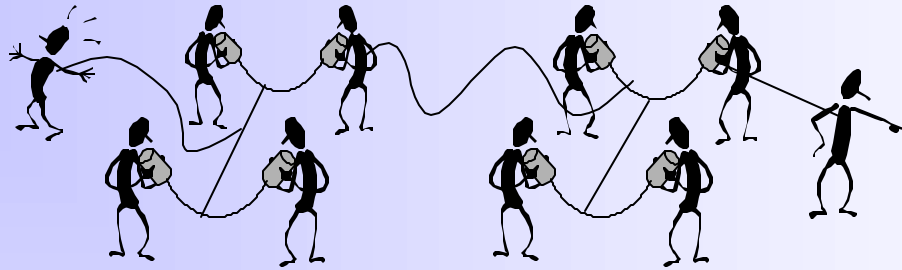
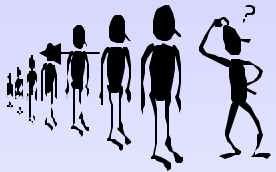


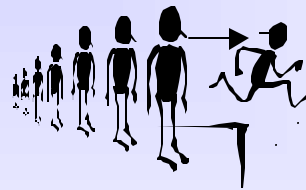
CLQ_API: Group Key Agreement API based on CLIQUES protocol suite



Formation



Member add



Member leave



Group fusion



Group fission

CLQ_API prerequisites

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

- ***group joins (single member)***
- ***group leaves (single member; voluntary)***
- ***partitions (leaves “en masse”)***
- ***node failures or disconnects (involuntary)***
- ***merges (heals)***

NOTE: the above is not an absolute req-t!

CLQ_API

- **clq_join** new member calls after getting context from GC
- **clq_proc_join** called by GC to hand over group context after updating key share
- **clq_update_ctx** each member calls as the last step of JOIN, LEAVE, MERGE or REFRESH; updates key
- **clq_leave** each member calls after receiving a LEAVE event
- **clq_refresh_key** any member can call (usually GC) to update its share
- **clq_update_key** GC and new member call during MERGE (1st stage)
- **clq_factor_out** all members call during MERGE (2nd stage)
- **clq_merge** new GC calls to merge groups (3rd stage)
- **clq_first_member** only called by “founding” member

CLQ_API

Group Controller

New Member

All Members

clq_proc_join

clq_join

clq_proc_join

clq_update_ctx

JOIN

Group Controller

Leaving Member

All Members

clq_leave

clq_leave

clq_update_ctx

LEAVE

CLQ_API

Group Controller

All Members

clq_refresh_key

clq_update_ctx

REKEY

Group Controller

New Members

Last New

All Members

clq_update_key

clq_update_key

clq_update_key

MERGE

clq_merge

clq_factor_out

clq_update_ctx

Last Slide

- λ Home page: <http://www.isi.edu/div7/CLIQUE>
- λ API code available on discretionary basis
- λ Will be unconditionally released soon
- λ INTERNET_DRAFT ready this week...
- λ Implementing centralized scheme as a point of comparison
- λ Integration with SPREAD nearing completion
- λ TOTEM integration underway
- λ Experimenting with different group sizes, geo. distribution
- λ Results to be published soon