

Dynamic Cryptographic Context Management (DCCM)

High Confidence Networks (HCN) PI Meeting
March 11, 1998

Trusted Information Systems, Inc.
David M. Balenson, Co-PI

Sponsored by the
High Confidence Networks Program
DARPA Contract No. F30602-97-C-0277
Hilarie Orman, DARPA, Program Manager
Lt. Brian Witten, USAF, COTR

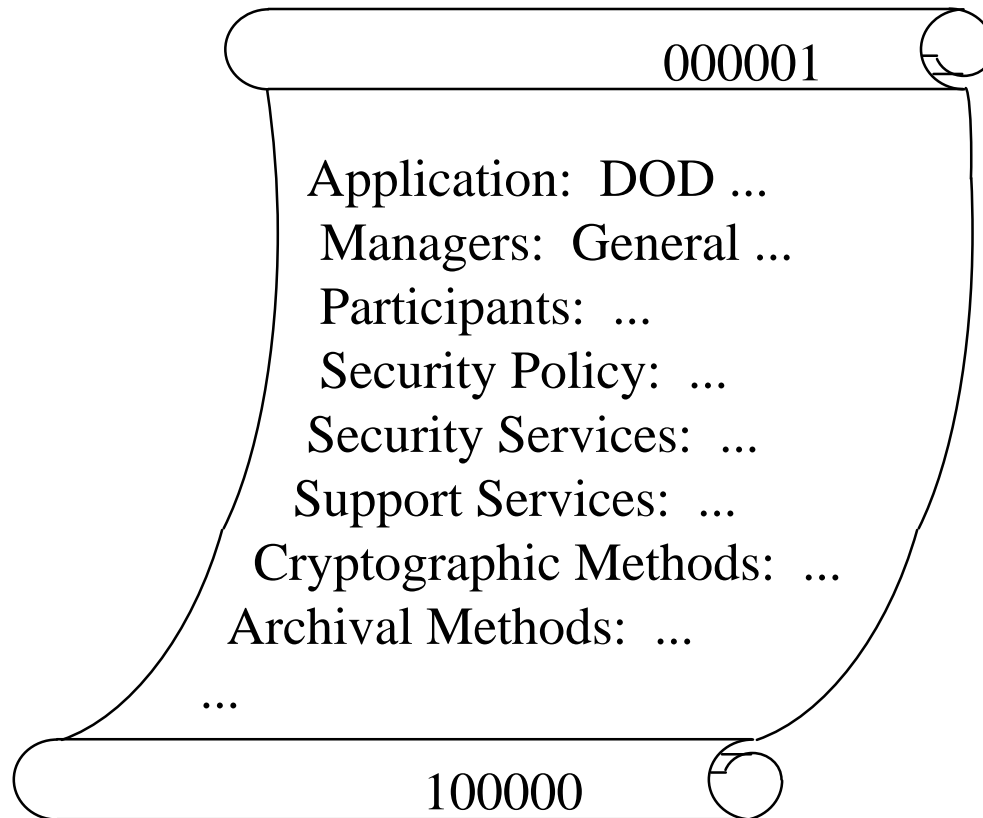
Presentation Outline

- Goals / objectives
- Tasks
- Timeline
- Multi-party application phases
- Group key establishment & rekey
- Expected results and capabilities

Project Goals / Objectives

- Security management for very large, dynamic, heterogeneous groups
 - military command and control, collaborative computing, war gaming, and conferencing w/ up to 100,000 group members
- Support creation and enforcement of dynamic security policies
 - managers, participants, security services, crypto methods, etc.
- Specify security policies, translate to cryptographic contexts, and negotiate contexts
- Establish group keys and change keys as group membership changes

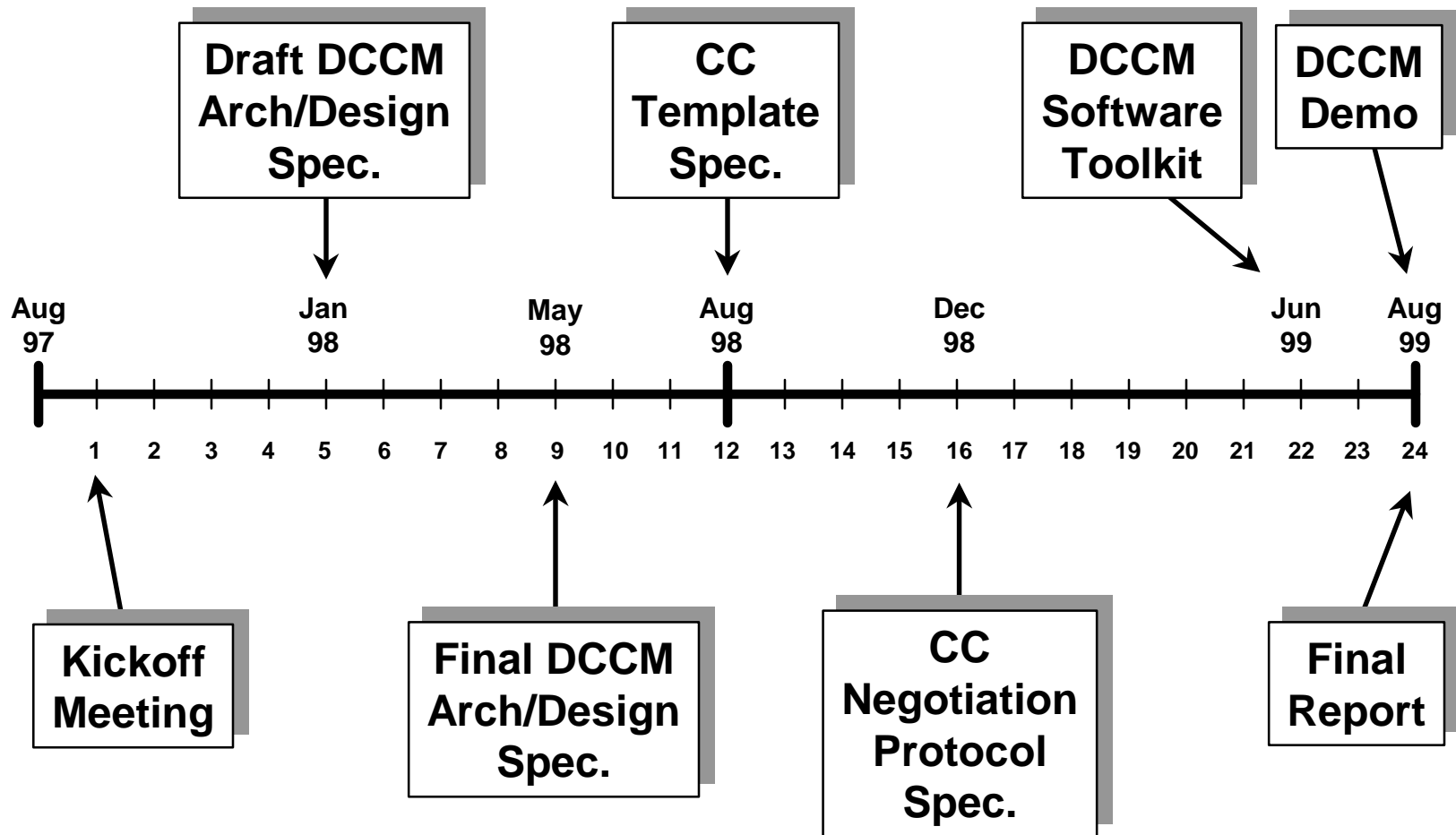
Cryptographic Context Template



Project Tasks

- Analysis tasks
 - security requirements, security policy language requirements, communications protocols, key management protocols for multi-party applications
- Specification tasks
 - system architecture/design, crypto context template, policy language and translation of crypto context, crypto context negotiation protocol, key management protocol for multi-party applications
- Software development & demonstration tasks
 - manager and user workstation software toolkit for multi-party applications

Project Timeline



Multi-Party Application Phases

- System/application/session initialization
 - translate security policy into crypto context
 - negotiate crypto context
- Group member initialization
 - authenticate public keys -- X.509v3 certificates, secure DNS
 - establish pairwise keys -- ISAKMP/OAKLEY
- Group key establishment & re-key
 - SKDC, Group DH, LKH, or OFT
- Group communications
 - Confidentiality -- IPsec, TLS, or application layer
 - Authentication -- MAC for group, signature for individual

Group Key Establishment & Re-key

- Simple linear methods -- Simple Key Distribution Center
 - scale poorly, but attractive for small to moderate groups
- Information-Theoretic
 - require exponential member space
- Group Diffie-Hellman
 - require slow public-key operations (linear)
 - attractive for small groups when distributed control needed
- Hierarchical -- LKH, OFT
 - scale best to very large groups

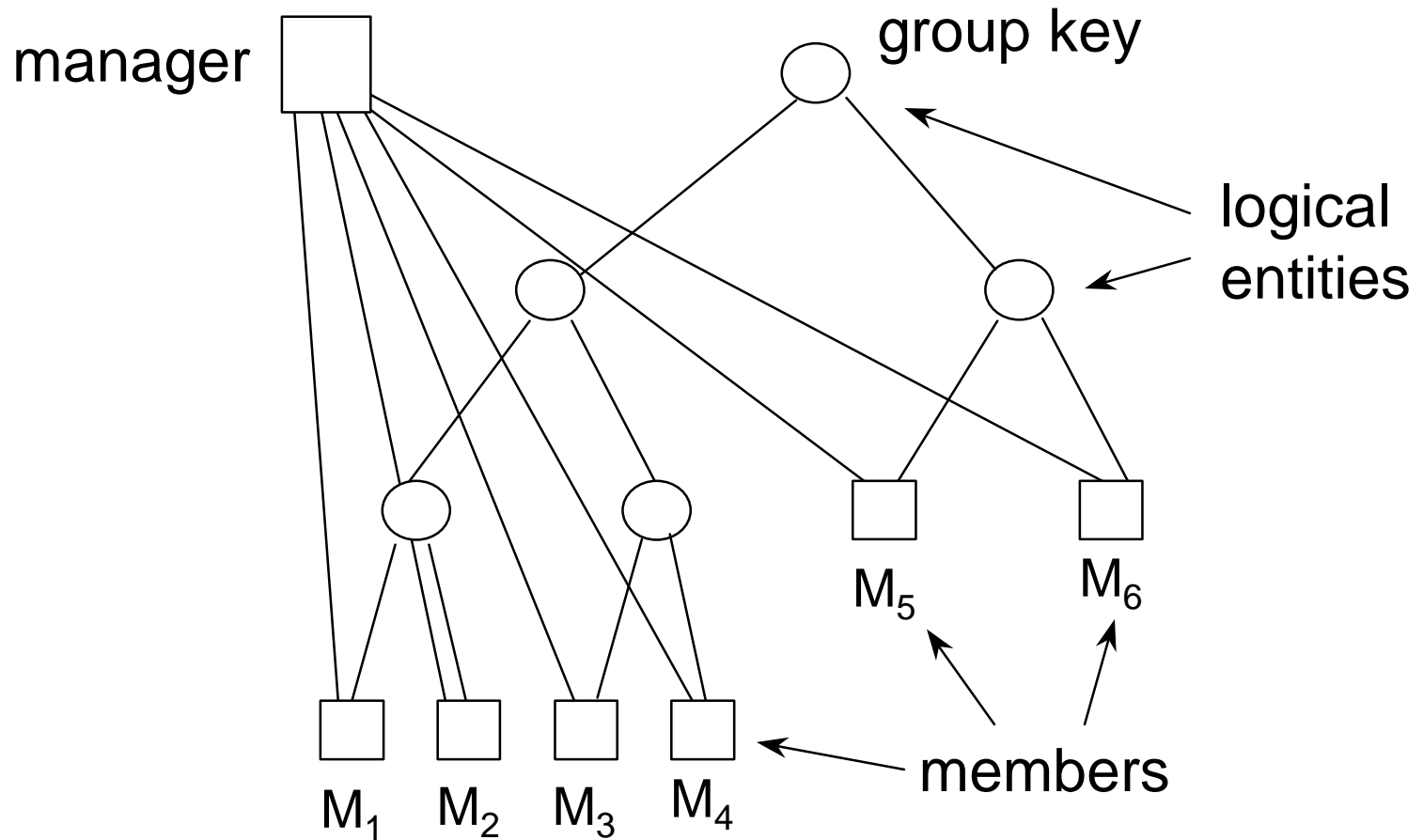
Logical Key Hierarchy (LKH)

- Wallner, Harder, Agee, NSA, 1997)
- Update keys via encrypting node keys down a tree with members at the leaves
- Time, space, broadcast scale logarithmically
- Simple security properties

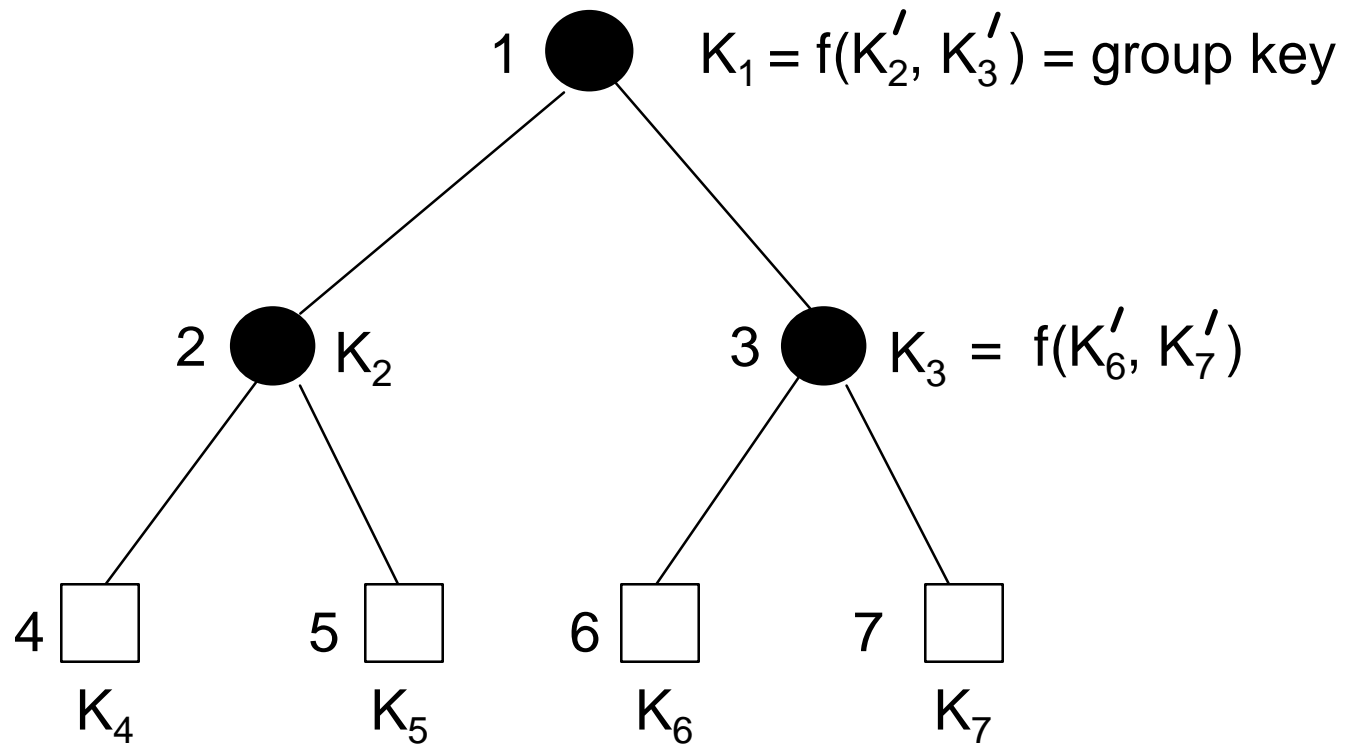
One-way Function Tree (OFT)

- McGrew, Sherman, TIS, 1997
- Novel application of one-way function trees
- Reduces number of broadcast bits for re-key

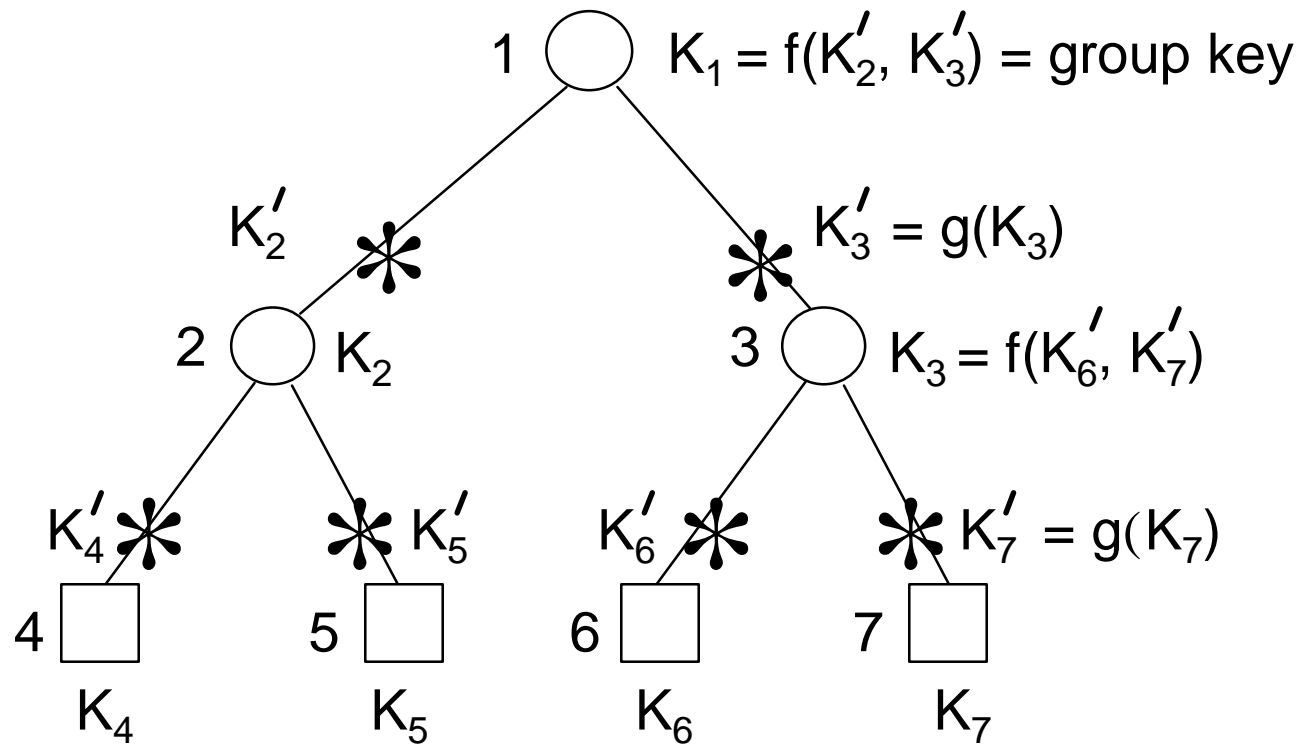
Hierarchical Model



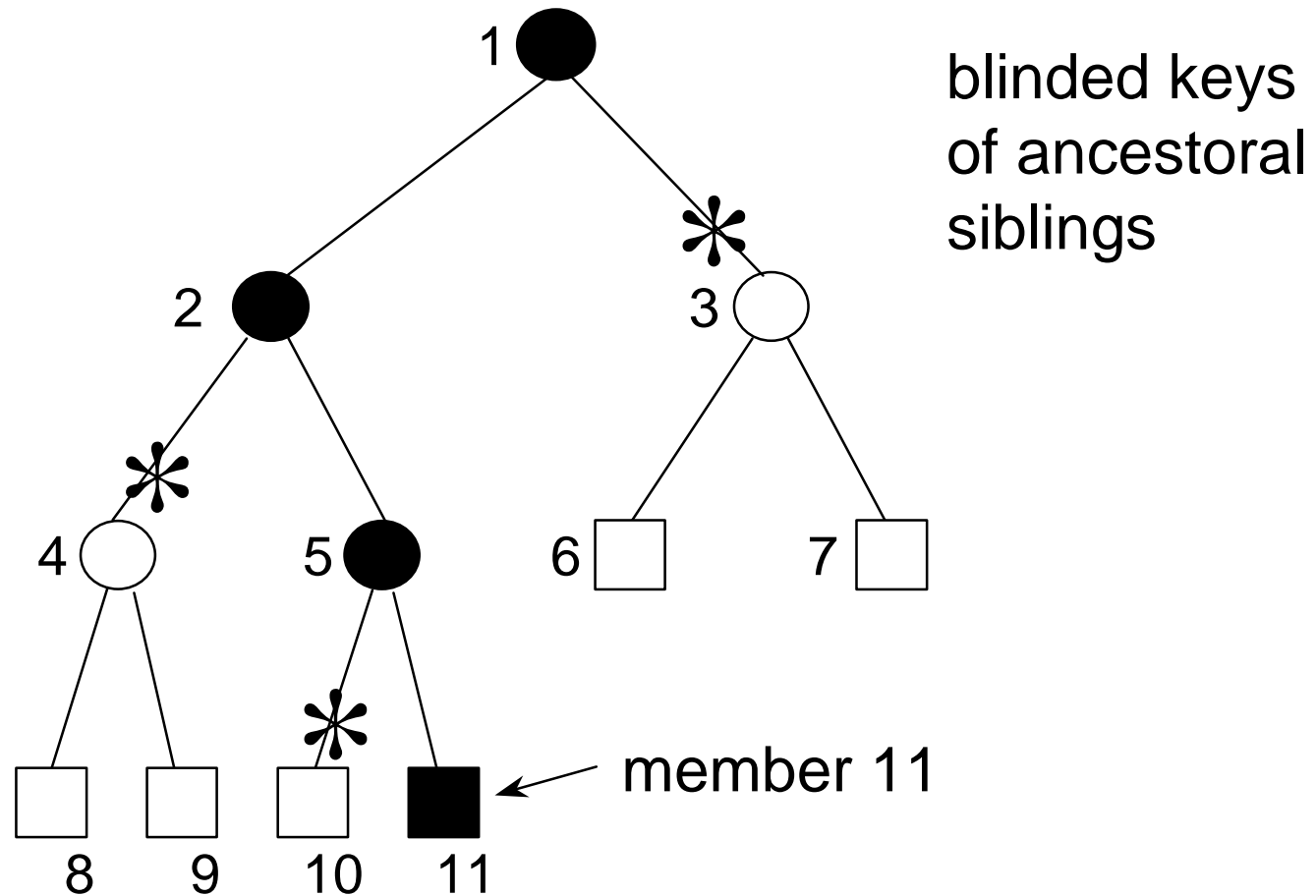
OFT Key Derivation - Node Keys



OFT Key Derivation - Blinded Node Keys



What a Member Needs to Know



Space Requirements & Broadcast Size

SPACE (# keys)

<u>Method</u>	<u>Manager</u>	<u>Member</u>
SKDC	n	2
LKH	$2n$	h
OFT	$2n$	h

BROADCAST SIZE (# keys)

<u>Method</u>	<u>Add</u>	<u>Evict</u>
SKDC	n	n
LKH	$2h$	$2h$
OFT	h	h

h = tree height, n = group size

Communication Size for Add/Evict

ADD (# keys)

<u>Method</u>	<u>Broadcast</u>	<u>Unicast</u>
SKDC	n	0
LKH	$2h$	0
OFT	2	h

EVICT (# keys)

<u>Method</u>	<u>Broadcast</u>	<u>Unicast</u>
SKDC	n	0
LKH	$2h$	0
OFT	h	0

h = tree height, n = group size

Expected Results and Capability

- Comprehensive architecture / system design for large, dynamic multi-party applications
- Multi-party cryptographic context template
- Multi-party security policy specification language and software translator
- Cryptographic context negotiation and establishment protocol and software
- Efficient methods for group key establishment and re-key