Review of CLIQUES: A New Approach to Group Key Agreement  
By Jeremy Miller

Goals of the Paper.

The goals of CLIQUES is to describe an efficient protocol for sharing a common group key among the members of the group while providing enough security to protect against passive attacks. The paper describes how to use Diffie-Hellman to efficiently create groups, add members to a group, remove the members from a group, fuse groups into a monolithic group and separate monolithic a group into smaller groups. The paper gives implementation details on how and why they used Diffie-Hellman to achieve these goals. The paper also describes different group keying techniques and gives why they chose one over another.

The CLIQUES group choose to use a partial contributory model of key distribution so that each member of a group will contributed some key data to the group's key. The partial contributory model allowed the existence of a group leader to facilitate easy addition and removal of group members and controlling authentication to the group. The use of the partial contributory model allowed the CLIQUES developers to create protocols that would allow any member of the group to become the “group leader”. This gave the protocol a distinction from other previously developed keying protocols. The paper also develops an Initial Key Agreement and a Auxiliary Key Agreement protocol. The Initial Key Agreement protocol is used when a groups is first formed or when a group is “leaderless” and a total rekeying of the group is necessary. The Auxiliary Key Agreement (AKA) is used when the group leader initiates a new addition or removal without having to do a total rekeying of all group members. The security property that is important to all AKA operations is key independence. Key independence is required so that new keys remain unattainable to former group members and old are undiscoverable by new members.

Things I liked about the paper.

The paper effectively communicates how to used Diffie-Hellman to implement a group key policy. The paper even includes references to others works on more specific group keying schemes. I particularly liked how the paper included to Ingearsson's and Steer's work and informed the reader about how and when these two differing protocol are more efficient than the CLIQUES protocol. The paper also hinted toward the possibility of an API for the CLIQUES protocol. This seems like a logical next step in the development of the protocol. It was surprising to me see a security paper that actually talks about the possibility of a implementation. However, the implementation of the CLIQUES protocol seems feasible due to the assumptions and constraints they placed on the protocol. I also liked how the papers authors identified further research and development areas for the proposed solution to group keying

Things I disliked about the paper.

I did not enjoy the extensive use of mathematical notation when a “Alice, Bob and Eve” example would have been easier to read and understand. The paper also assumes that all from of attacks on the protocol will be passive attacks. I find this to be a dangerous assumption and the group should have done some work on prevent active attacks.