In this paper, the authors proposed a protocol suite called CLIQUES to allow key agreement in dynamic groups. CLIQUES extends the well-known Diffie-Hellman key agreement, uses partially contributory model, and has group controller in the protocol. Group communication is nothing similar to two-party communication since it starts, the group mutates, and no well-defined end might happen. Due to this group dynamics, key agreement is especially important for secure group communication.

There are Initial Key Agreement (IKA) and Auxiliary Key Agreement (AKA) operations. IKA occurs at the time of group genesis, and refers to the initial group key agreement. Whereas AKA includes all subsequent key agreement operations. The security of the IKA is more important than its overhead costs. However, it is best to minimize the overhead of IKA since key agreement must come before any kind of secure group communication. The AKA operations has the security property of key independence. That is, previous used group keys must not be discovered by new group members. And new keys must remain out of reach from former group members. Here the authors only consider passive known-key attacks on short-term session keys. So the attacker in the IKA/AKA protocols can be an outsider or a quasi-insider. The AKA operations include single member operations as member addition and member exclusion, subgroup operations include group addition as mass join and group fusion, and group exclusion as mass leave, group division, and group fission.

The IKA protocol in CLIQUES protocol is called GDH.2. The GDH.2 protocol executes in two stages. In the first stage the n-1 rounds of member contributions are collected from group members. And in the second stage the group controller will broadcast the group keying material for group members to compute the final group key. The member addition protocol can support a floating group controller that let the new member to become the new group controller or a fixed group controller that let the group controller be the same. Mass join can be done by adding multiple members that runs single-member addition protocol consecutively. However, it is not an efficient way because the overhead is very high. The better approach the authors presented is to chain the member addition protocol and only making one broadcast at the end.

This paper is more of a theoretical paper that used DH protocol as a cornerstone to effectively implement group key agreement. The authors pointed out a lot of previously related work about other protocols that extends DH protocol. They stated why the proposed CLIQUES protocol is more suitable for dynamic groups and had some comparison between the protocols. In the future work part, the authors mentioned a lot of the remaining issues including a better group fusion protocol, key integrity provisions, member authentication, scaling issues, and API definition. These are all interesting aspects to think about. I am especially concerned about the scaling issue of CLIQUES because it is clear that CLIQUES is not scalable to large size groups.