Secure Group Key Exchange, Revisited
Mike Burmester
Florida State University

Group Key Exchange (GKE) protocols are a generalization of two-party KE protocols, such as the Diffie-Hellman KE, to groups of $n \geq 2$ users. Recently Katz and Yung described a compiler that transforms a GKE protocol into an authenticated GKE (AKE) protocol. In particular, they showed how the cycle-based version of the Burmester-Desmedt GKE (BD-I) can be used to get an AKE with constant rounds (3) and $O(n)$ communication and computation complexity (per user). The problem with this solution is that it is not scalable: the complexity per user can be very large. In this talk we shall look at the issues involved in KE and GKE, from both a security point of view and a complexity point of view. We will review the two Burmester-Desmedt GKE protocols: the cycle-based protocol (BD-I) and a tree-based protocol (BD-II). Then we shall briefly overview other authenticated GKE proposed in the literature. Finally we shall show how to design a scalable compiler for tree-based GKE protocols and use it to get an authenticated version of BD-II that requires only 3 rounds and has $O(\log n)$ complexity.