1125-94-2922 **Kashi Neupane*** (knneupane@ung.edu). *One-Round Authenticated Group Key Establishment from Multilinear Mappings.*

In this paper, we propose a one-round authenticated group key establishment protocol. Our protocol is based on Graded Decisional Diffie-Hellman assumption, and it requires timestamps. The resulting solution is in the random oracle model, builds on a multi-linear map, and offers integrity as well as strong entity authentication. (Received September 20, 2016)