1116-94-2581 **Kashi N Neupane*** (knneupane@ung.edu), University of North Georiga, Department of Mathematics, Gainseville Campus, Gainseville, GA 30503. *Long-term secure two-round group key establishment from pairings.*

In 2007, Bohli et al. introduced the concept of long-term security as resistance against attacks even if later, after completion of the protocol some security assumptions become invalid, and proposed a three-round long-term secure two-party key establishment protocol. Building on a two-party solution of Bohli et al., we present an authenticated two-round group key establishment protocol which remains secure if either a Computational Bilinear Diffie Hellman problem is hard or a server, who shares a symmetric key with each user, is uncorrupted. (Received September 22, 2015)