1077-94-1635 **K N Neupane*** (kneupane@fau.edu), Department of Mathematical Sciences, Florida Atlantic University, 777 Glades Road, Boca Raton, FL 33431, and **R Steinwandt**, Department of Mathematical Science, Florida Atlantic University, 777 Glades Road, Boca Raton, FL 33431.
Communication-efficient 2-round group key establishment from pairings.

In a recent preprint, Vivek et al. propose a compiler to transform a passively secure 3-party key establishment to a *passively* secure group key establishment. To achieve *active* security, they apply this compiler to Joux's protocol and apply a construction by Katz and Yung, resulting in a 3-round group key establishment.

In this paper we show how Joux's protocol can be extended to an *actively* secure group key establishment with two rounds. The resulting solution is in the standard model, builds on a bilinear Diffie-Hellman assumption and offers forward security as well as strong entity authentication. If strong entity authentication is not required, then one half of the participants does not have to send any message in the second round, which may be of interest for scenarios where communication efficiency is a main concern. (Received September 20, 2011)