1056-12-942 **Daniel C. Smith*** (smithdc@indiana.edu), Indiana University, Department of Mathematics, 831 East 3rd St, Bloomington, IN 47405. *The Effect of Projection on the Symmetry of the SFLASH Attack.*

Dubois, Fouque, Shamir, and Stern published an attack in 2007 which breaks SFLASH and many other multivariate public key schemes similar to C^{*-}. The attack relies on a multiplicative symmetry exhibited by the hidden internal field map of the encryption function. Ding later suggested projection, the method previously called "fixing," as a means of preventing the attack. We present a detailed analysis of the effect of projection on the multiplicative symmetry including a proof of Ding's suggestion as well as the discovery of a new symmetry preserved under projection. (Received September 18, 2009)