1046-12-1387 **Daniel C Smith*** (smithdc@indiana.edu), Daniel C Smith, Indiana University, Department of Mathematics, Bloomington, IN 47405. *The Limits of the Attack on SFLASH.*

In 2003, the NESSIE consortium selected SFLASH as a recommended public key signature scheme. In 2007, Dubois, Fouque, Shamir, and Stern discovered an attack which completely breaks the signature scheme. This attack undermines not only the security of SFLASH and C^{*-} but the security of other multivariate public key systems which are designed with a similar philosophy. The attack relies on a multiplicative symmetry of the encryption mapping. We give a comprehensive classification of encryption mappings with this multiplicative symmetry, prove that the method of projection, as suggested by Ding, safeguards the scheme from the attack of Dubois et al., and show that the attack cannot be applied to the more general HFE setting. (Received September 15, 2008)