1086-12-2786 **Daniel C Smith*** (daniel-c.smith@louisville.edu). *Differential Invariants in Cryptography.*

The versatility of differential attacks in multivariate cryptography is a point of serious concern as the cryptographic community explores potential candidates for a quantum-resistant cryptosystems. We present some cryptosystems which have been broken with the discovery of techniques for solving discrete differential equations by finding anomalous differential invariants. We conclude proposing a route to providing a metric for differential invariant security. (Received September 25, 2012)