1092-12-91 **Ray Perlner*** (ray.perlner@nist.gov) and **Daniel Smith** (dcsmit11@louisville.edu). *A Classification of Differential Invariants for Multivariate Post-Quantum Cryptosystems.*

Multivariate Public Key Cryptography is one of the most promising candidates for designing public key cryptosystems which remain secure in the quantum model of computation. Nonetheless, while a few multivariate systems remain secure after years of cryptanalysis, many have fallen to a surprisingly small pool of cryptanalytic techniques.

This talk summarizes our research, most recently published at PQCrypto 2013, aimed at formalizing requirements for multivariate cryptosystems to resist broad classes of known attacks. The PQCrypto paper focused in particular on attacks based on invariant subspaces derived from the discrete differential of the quadratic maps, which are the public keys of existing multivariate schemes. The most notable cryptosystem which fell to this class of attacks was the balanced oil-and-vinegar scheme. Our research addresses the possibility of similar attacks in the case of big-field schemes, such as the currently unbroken scheme, pSFLASH. (Received July 31, 2013)