Cryptology ePrint Archive: Report 2013/173

On the Classification of Differential Invariants for Multivariate Post-Quantum Cryptosystems"

Ray Perlner and Daniel Smith-Tone

Abstract: Multivariate Public Key Cryptography(MPKC) has become one of a few options for security in the quantum model of computing. Though a few multivariate systems have resisted years of effort from the cryptanalytic community, many such systems have fallen to a surprisingly small pool of techniques. There have been several recent attempts at formalizing more robust security arguments in this venue with varying degrees of applicability. We present an extension of one such recent measure of security against a differential adversary which has the benefit of being immediately applicable in a general setting on unmodified multivariate schemes.

Category / Keywords: public-key cryptography / Matsumoto-Imai, multivariate public key cryptography, differential, symmetry

Date: received 26 Mar 2013

Contact author: daniel smith at nist gov

Available formats: PDF | BibTeX Citation

Version: 20130330:224740 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]