The Department of Mathematical Sciences

Taft Lecture Series

presents

Daniel Smith-Tone

The National Institute of Standards and Technology

Friday, April 8, 2016
3:30 – 4:30 pm
Charles Phelps Taft Research Center
Edwards I, Suite 1110

Symmetry in Differential Analysis in Multivariate Public Key Cryptography

Since the discovery by Peter Shor in the mid-1990s that factoring and computing discrete logarithms are feasible tasks for a large quantum computer, a large international community has arisen, devoted to the challenge of securing information in a quantum computing society. These cryptographic zealots have christened this new science "Post-Quantum Cryptography," eliciting images of a post-apocalyptic world in which quantum computing machines reign supreme.

Multivariate public key cryptosystems (MPKCs) form one among a few families of asymmetric schemes that seem to resist quantum attack. A critical challenge is that of resistance to new techniques of cryptanalysis.

In this talk we provide a partial (and not yet fully satisfactory) answer to this question. We begin by reviewing the history of MPKCs, including specific examples of several important attacks. We will show that these attacks involve solving certain functional equations relating to a notion of a differential of the public key. We formulate a program for proving the resistance of a scheme against a differential adversary. As an application, we prove that a notable scheme, HFE- provably resists differential cryptanalysis in this model.

TAFT research center

UNIVERSITY OF Cincinnati