Optimal algebraic manipulation detection codes and difference families

Douglas R. Stinson, University of Waterloo

We present a mathematical analysis of (optimal) algebraic manipulation detection (AMD) codes, which have several cryptographic applications.
We prove several lower bounds on the success probability of an adversary and we then give some combinatorial characterizations of AMD codes that meet the bounds with equality.
These characterizations involve various types of generalized difference families. Constructing these difference families is an interesting problem in its own right.
In particular, the problem of constructing "strong external difference families" has attracted a considerable amount of attention by several researchers in the last few months. We discuss the current state of knowledge for this interesting problem.

This talk is based on joint work with Bill Martin and Maura Paterson