1116-05-1313 **Douglas R Stinson*** (dstinson@uwaterloo.ca) and **Maura B Paterson**. *Characterisations of Optimal Algebraic Manipulation Detection Codes.*

Algebraic manipulation detection (AMD) codes are algebraic/combinatorial structures that are closely related to difference sets. They were defined as a generalisation and abstraction of techniques previously used in constructing robust secret sharing schemes, and their use has been proposed for a range of other cryptographic applications. In this talk we consider lower bounds on the success probability of an adversary in attacking an AMD code, as well as combinatorial characterisations of AMD codes meeting these bounds with equality. (Received September 18, 2015)