MAURA PATERSON, Birkbeck, University of London

Authentication codes with perfect secrecy and algebraic manipulation detection codes

The construction and analysis of authentication codes for providing authentication in an unconditionally secure setting is a long-standing practical application of design theory. Algebraic manipulation detection (AMD) codes were introduced by Cramer et al. in EUROCRYPT 2008 in order to apply ideas used in the construction of robust secret sharing schemes to more general cryptographic systems. In this talk we examine automorphism groups of authentication codes and show that AMD codes can be viewed as a special case of splitting authentication codes with perfect secrecy.

This talk is based on joint work with Doug Stinson.