Analysis of Algebraic Ciphers for Advanced Cryptographic Applications

Carlos Cid

Royal Holloway, University of London, UK

Recent years have seen the proposal of several custom designs of symmetric-key ciphers for advanced applications, such as Zero-Knowledge proofs and Multi-Party Computation. These ciphers aim to minimise the complexity of some basic operation, eg. the number of multiplications on a large field, in order to improve performance for particular applications. Given the often simple algebraic structure of these ciphers, they may be particularly vulnerable to algebraic attacks, a class of attacks that is typically not considered to be competitive with more traditional types of block cipher cryptanalysis (eg. differential cryptanalysis). In this talk, we will discuss the algebraic analysis of selected algebraic ciphers.

Information Security Group, Department of Mathematics, Royal Holloway, University of London, Egham, Surrey, TW20 0EX, UK
Carlos.Cid@rhul.ac.uk