Low-cost arithmetic in extended finite fields using structured matrices

Anwar Hasan
University of Waterloo, Canada

Abstract. For cryptography and coding, finite fields are used extensively. Some public key cryptosystems rely on very large prime and/or extended finite fields. Performance of such cryptosystems depends on the efficiency of arithmetic over the underlying finite field. In this talk, we look into the formulation of arithmetic operations over extended finite fields as matrix operations over a sub-field. We consider a variety of bases for representing the field elements and show their connections to some structured matrices for low-cost arithmetic.