CORR 99-64

On the Interpolation Attacks on Block Ciphers

A.M. Youssef & G. Gong

Abstract The complexity of interpolation attacks on block ciphers depends on the degree of the polynomial approximation and/or on the number of terms in the polynomial approximation expression. In some situations, the round function or the S-boxes of the block cipher are expressed explicitly in terms of algebraic function, yet in many other occasions the S-boxes are expressed in terms of their Boolean function representation. In this case, the cryptanalyst has to evaluate the algebraic description of the S-boxes or the round function using the Lagrange interpolation formula. A natural question is what is the effect of the choice of the irreducible polynomial. Another question is whether or not there exists a simple linear transformation on the input or output bits of the S-boxes (or the round function) such that the resulting polynomial has a less degree or smaller number of non-zero coefficients. In this paper we give an answer to these questions. We also present an explicit relation between the Lagrange interpolation formula and the Galois Field Fourier Transform.