# CORR 2000-50

## Spectral Domain Analysis of Correlation Immune and Resilient Boolean Functions

**Palash Sarkar**

**Abstract** In this paper we prove a general result on the Walsh Transform of an arbitrary Boolean function. As a consequence, we obtain several divisbility results on the Walsh Transform of correlation immune and resilient Boolean functions. This allows us to improve upper bounds on the nonlinearity of correlation immune and resilient Boolean functions. Also we provide new necessary conditions on the algebraic normal form of correlation immune/resilient functions attaining the maximum possible nonlinearity.

**Keywords** stream ciphers, Boolean function, correlation immunity, resiliency, nonlinearity, algebraic degree.