CORR 2001-27

Cross-Correlation Analysis of Cryptographically Useful Boolean Functions and S-boxes

Palash Sarkar & Subhamoy Maitra

Abstract We use the cross-correlation function as a fundamental tool to study cryptographic properties of Boolean functions. This provides a unified treatment of a large section of Boolean function literature. In the process we generalize old results and obtain new characterizations of cryptographic properties. In particular, new characterizations of bent functions and functions satisfying propagation characteristics are obtained in terms of the cross-correlation and auto-correlation properties of sub functions. The exact values is obtained for a cryptographically important class of functions. Finally we study the suitability of S-boxes in stream ciphers and conclude that currently known constructions for S-boxes have potential weaknesses for such applications.

Keywords cross-correlation, Boolean functions, S-box, bent function, propagation characteristics, resiliency.