Analyzing the Bounds of Transparency Order of Boolean Functions

Mayasar Ahmad Dar* and Deepmala Sharma

Department of Mathematics, National Institute of technology, Raipur, Chhattisgarh, India

*Corresponding authors: darmayasar42@gmail.com, deepsha.maths@nitrr.ac.in

ABSTRACT

Transparency order is considered to be a cryptographically significant property having impact on the security of a cryptosystem. The notion of transparency order characterizes the resilience of cryptographic algorithms against differential power analysis attacks. Differential power analysis is a form of side-channel analysis, which studies the power consumption of cryptographic hardware devices. As the only nonlinear part in many ciphers, the S-box is crucial for the security of the cipher, and its cryptographic properties should be good. For assessing behavior of an S-box against side-channel analysis, several properties were proposed; the transparency order is one among them. The challenge is that highly nonlinear S-boxes have high transparency order, implying they are more susceptible to differential power analysis attacks, while linear S-boxes are good in terms of transparency order but cannot be used for other cryptographic reasons. Differential power analysis relies on the leakages from physical hardware implementations and is more efficient than the differential or linear cryptanalysis. It should be noted that a proper choice of transparency order can lead to less overheads in the various countermeasures. If all other cryptographic properties of two functions are equivalent, then a designer can choose a function with a better transparency order. A low transparency order is considered to be good. The transparency order and nonlinearity cannot be both good in the same time. However, given some nonlinearity, we can choose a function with good transparency order. So far, a little attempt has been made to analyze theoretically the transparency order and constructions related to the transparency order. In this paper, we study the transparency order of Boolean functions and obtain the various results on the bounds of transparency order of Boolean functions.

Keywords: Transparency Order, Boolean functions, Cross correlation

DOI: 10.21467/abstracts.158 ISBN: 978-81-965621-0-6 (eBook)