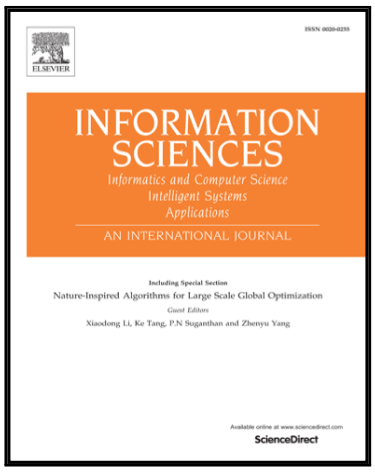

Improving the lower bound on the maximum nonlinearity of 1-resilient Boolean functions and designing functions satisfying all cryptographic criteria

WeiGuo Zhang, Enes Pasalic

PII: S0020-0255(16)31154-9
DOI: 10.1016/j.ins.2016.10.001
Reference: INS 12560

To appear in: *Information Sciences*

Received date: 19 June 2015
Revised date: 28 September 2016
Accepted date: 2 October 2016

Please cite this article as: WeiGuo Zhang, Enes Pasalic, Improving the lower bound on the maximum nonlinearity of 1-resilient Boolean functions and designing functions satisfying all cryptographic criteria, *Information Sciences* (2016), doi: 10.1016/j.ins.2016.10.001

Improving the lower bound on the maximum nonlinearity of 1-resilient Boolean functions and designing functions satisfying all cryptographic criteria

WeiGuo Zhang*
1. ISN Laboratory, Xidian University, Xi'an 710071, China
2. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
e-mail: zwg@xidian.edu.cn

Enes Pasalic
University of Primorska, FAMNIT, Koper 6000, Slovenia
e-mail: enes.pasalic6@gmail.com

Abstract

In this article we improve the lower bound on the maximum nonlinearity of 1-resilient Boolean functions, for n even, by proposing a method of constructing this class of functions attaining the best nonlinearity currently known. Thus for the first time, at least for small values of n, the upper bound on nonlinearity can be reached in a deterministic manner in difference to some heuristic search methods proposed previously. The nonlinearity of these functions is extremely close to the maximum nonlinearity attained by bent functions and it might be the case that this is the highest possible nonlinearity of 1-resilient functions. Apart form this theoretical contribution, it turns out that the cryptographic properties of these functions are overall good apart from their moderate resistance to fast algebraic attacks (FAA). This weakness is repaired by a suitable modification of the original functions giving a class of balanced functions with almost optimal resistance to FAA whose nonlinearity is better than the nonlinearity of other methods.

Keywords: Boolean functions, nonlinearity, resiliency, algebraic immunity, stream ciphers.

1 Introduction

In a modern design of certain stream cipher encryption schemes there are many cryptographic criteria that affect the choice of Boolean functions commonly used for the purpose

*Corresponding author; Email: zwg@xidian.edu.cn