Accepted Manuscript

Constructions of balanced odd-variable rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity

Lei Sun, Fang-Wei Fu

PII: S0304-3975(18)30278-0
DOI: https://doi.org/10.1016/j.tcs.2018.04.040
Reference: TCS 11570

To appear in: *Theoretical Computer Science*

Received date: 4 November 2016
Revised date: 28 February 2018
Accepted date: 18 April 2018

Please cite this article in press as: L. Sun, F.-W. Fu, Constructions of balanced odd-variable rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity, *Theoret. Comput. Sci.* (2018), https://doi.org/10.1016/j.tcs.2018.04.040

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

Highlights

- We propose a new class of rotation symmetric Boolean functions(RSBFs) having almost all of the main cryptographic properties: balancedness, high algebraic degree,optimal algebraic immunity, high nonlinearity.
- The nonlinearity of the proposed RSBFs is much higher than all the previously obtained RSBFs with optimal algebraic immunity.
- The proposed RSBFs have good behavior against fast algebraic attacks at least for small numbers of input variables.

Download English Version:

https://daneshyari.com/en/article/6875418

Download Persian Version:

https://daneshyari.com/article/6875418

Daneshyari.com