Cryptology ePrint Archive: Report 2011/503

On the influence of the algebraic degree of $F^{−1}$ on the algebraic degree of $G \circ F$

Christina Boura and Anne Canteaut

Abstract: We present a study on the algebraic degree of iterated permutations seen as multivari- ate polynomials. Our main result shows that this degree depends on the algebraic degree of the inverse of the permutation which is iterated. This result is also extended to non-injective balanced vectorial functions where the relevant quantity is the minimal degree of the inverse of a permutation expanding the function. This property has consequences in symmetric cryptography since several attacks or distinguishers exploit a low algebraic degree, like higher-order differential attacks, cube attacks and cube testers, or algebraic attacks. Here, we present some applications of this improved bound to a higher-degree variant of the block cipher KN , to the block cipher Rijndael-256 and to the inner permutations of the hash functions ECHO and JH.

Category / Keywords: secret-key cryptography /

Date: received 15 Sep 2011, last revised 18 Sep 2011

Contact author: christina boura at inria fr

Available formats: PDF | BibTeX Citation

Version: 20110918:064101 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]