Cryptology ePrint Archive: Report 2011/023

Improved zero-sum distinguisher for full round Keccak-f permutation

Ming Duan and Xuajia Lai

Abstract: K$\textsc{eccak}$ is one of the five hash functions selected for the final round of the SHA-3 competition and its inner primitive is a permutation called K$\textsc{eccak}$-f. In this paper, we find that for the inverse of the only one nonlinear transformation of K$\textsc{eccak}$-f, the algebraic degrees of any output coordinate and of the product of any two output coordinates are both 3 and also 2 less than its size 5. Combining the observation with a proposition from an upper bound on the degree of iterated permutations, we improve the zero-sum distinguisher of full 24 rounds K$\textsc{eccak}$-f permutation by lowering the size of the zero-sum partition from 2^{1590} to 2^{1579}.

Category / Keywords: secret-key cryptography / hash functions, higher order differentials, algebraic degree, zero-sum, SHA-3.

Date: received 12 Jan 2011

Contact author: mduan at sjtu edu cn; lai-xj@cs sjtu edu cn

Available formats: PDF | BibTeX Citation

Version: 20110114:041641 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]