Cryptology ePrint Archive: Report 2011/017

New Impossible Differential Attacks of Reduced-Round Camellia-192 and Camellia-256

Jiazhe Chen and Keting Jia and Hongbo Yu and Xiaoyun Wang

Abstract: Camellia is a block cipher selected as a standard by ISO/IEC, which has been analyzed by a number of cryptanalysts. In this paper, we propose several 6-round impossible differential paths of Camellia with the FL/FL^{-1} layer in the middle of them. With the impossible differential and a well-organized precomputational table, impossible differential attacks on 10-round Camellia-192 and 11-round Camellia-256 are given, and the time complexity are 2^{175} and $2^{206.8}$ respectively. An impossible differential attack on 15-round Camellia-256 without FL/FL^{-1} layers and whitening is also be given, which needs about $2^{236.1}$ encryptions. To the best of our knowledge, these are the best cryptanalytic results of Camellia-192/-256 with FL/FL^{-1} layers and Camellia-256 without FL/FL^{-1} layers to date.

Category / Keywords: Camellia Block Cipher, Cryptanalysis, Impossible Differential Path, Impossible Differential Attack

Date: received 9 Jan 2011, last revised 19 Jan 2011

Contact author: jiazhechen at gmail com