Cryptology ePrint Archive: Report 2011/524

Security of Reduced-Round Camellia against Impossible Differential Attack

Leibo Li, Jiazhe Chen and Xiaoyun Wang

Abstract: Camellia is one of the widely used block ciphers, which has been selected as an international standard by ISO/IEC. By using some interesting properties of FL/FL^{-1} functions, we introduce new 7-round impossible differentials of Camellia for weak keys, which can be used to attack reduced-round Camellia under weak-key setting. The weak keys that work for the impossible differential take 3/4 of the whole key space, therefore, we can further get rid of the weak-key assumption and leverage the attacks to all keys by utilizing a method that is called \emph{the multiplied method}. As a result, for the whole key space, 10-round Camellia-128, 11-round Camellia-192 and 12-round Camellia-256 can be attacked with about 2^{120}, 2^{184} and 2^{240} encryptions, respectively. In addition, we are able to extend the attacks to 12-round Camellia-192 and 14-round Camellia-256 which include two FL/FL^{-1} layers, provided that the attacks do not have to be started from the first round.

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

Date: received 24 Sep 2011, last revised 14 Nov 2011

Contact author: lileibo at mail sdu edu cn

Available formats: PDF | BibTeX Citation

Version: 20111114:072307 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]