Cryptology ePrint Archive: Report 2011/163

Improved Integral Attacks on Reduced Round Camellia

Yanjun Li, Wenling Wu, Liting Zhang and Lei Zhang

Abstract: In this paper a method is presented to extend the length of integral distinguisher of Feistel-SP structure, based on which a new 8-round distinguisher of Camellia is proposed. Moreover, we improve integral attacks on reduced round Camellia without FL/FL^{-1}. We attack 11-round Camellia-128 with the data complexity of 2^{120} and the time complexity of 2^{125.5}, and 12-round Camellia-256 with the data complexity of 2^{120} and the time complexity of 2^{214.3}. The result is the best one of integral attacks on reduced round Camellia so far.

Category / Keywords: secret-key cryptography / block ciphers, cryptanalysis, secret-key cryptography

Date: received 1 Apr 2011

Contact author: liyjwuyh at 163 com

Available formats: PDF | BibTeX Citation

Version: 20110404:082229 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]