

# Cryptology ePrint Archive: Report 2011/671

## Improved Results on Impossible Differential Cryptanalysis of Reduced-Round Camellia-192/256

*Ya Liu and Dawu Gu and Zhiqiang Liu and Wei Li and Ying Man*

**Abstract:** As an international standard adopted by ISO/IEC, the block cipher Camellia has been used in various cryptographic applications. In this paper, we reevaluate the security of Camellia against impossible differential cryptanalysis. Specifically, we propose several 7-round impossible differentials with the  $F_L/FL^{-1}$  layers. Based on them, we mount impossible differential attacks on 11-round Camellia-192 and 12-round Camellia-256. The data complexities of our attacks on 11-round Camellia-192 and 12-round Camellia-256 are about  $2^{120}$  chosen plaintexts and  $2^{119.8}$  chosen plaintexts, respectively. The corresponding time complexities are approximately  $2^{167.1}$  11-round encryptions and  $2^{220.87}$  12-round encryptions. As far as we know, our attacks are  $2^{16.9}$  times and  $2^{19.13}$  times faster than the previously best known ones but have slightly more data.

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

**Date:** received 10 Dec 2011, last revised 21 Dec 2011

**Contact author:** liuya0611 at sjtu edu cn

**Available formats:** [PDF](#) | [BibTeX Citation](#)

**Note:** We have revised some minor mistakes.

**Version:** 20111222:052321 ([All versions of this report](#))

**Discussion forum:** [Show discussion](#) | [Start new discussion](#)

---

[ [Cryptology ePrint archive](#) ]