

# Cryptography ePrint Archive: Report 2011/661

## New Impossible Differential Attacks on Camellia

*Dongxia Bai and Leibo Li*

**Abstract:** Camellia is one of the most worldwide used block ciphers, which has been selected as a standard by ISO/IEC. In this paper, we propose several new 7-round impossible differentials of Camellia with 2  $F_L/FL^{-1}$  layers, which turn out to be the first 7-round impossible differentials with 2  $F_L/FL^{-1}$  layers. Combined with some basic techniques including the early abort approach and the key schedule consideration, we achieve the impossible differential attacks on 11-round Camellia-128, 11-round Camellia-192, 12-round Camellia-192, and 14-round Camellia-256, and the time complexity are  $2^{123.6}$ ,  $2^{121.7}$ ,  $2^{171.4}$  and  $2^{238.2}$  respectively. As far as we know, these are the best results against the reduced-round variants of Camellia. Especially, we give the first attack on 11-round Camellia-128 reduced version with  $F_L/FL^{-1}$  layers.

**Category / Keywords:** secret-key cryptography / Camellia, Impossible Differential, Cryptanalysis, Impossible Differential Attack.

**Date:** received 7 Dec 2011

**Contact author:** baidx10 at mails tsinghua edu cn

**Available formats:** [Postscript \(PS\)](#) | [Compressed Postscript \(PS.GZ\)](#) | [PDF](#) | [BibTeX Citation](#)

**Version:** 20111209:210208 ([All versions of this report](#))

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

---

[ [Cryptography ePrint archive](#) ]