# Cryptology ePrint Archive: Report 2011/115

**Multiple Differential Cryptanalysis: Theory and Practice (Corrected)**

*Céline Blondeau and Benoît Gérard*

**Abstract:** Differential cryptanalysis is a well-known statistical attack on block ciphers. We present here a generalisation of this attack called multiple differential cryptanalysis. We study the data complexity, the time complexity and the success probability of such an attack and we experimentally validate our formulas on a reduced version of PRESENT. Finally, we propose a multiple differential cryptanalysis on 18-round PRESENT for both 80-bit and 128-bit master keys.

**Category / Keywords:** secret-key cryptography / iterative block cipher, multiple differential cryptanalysis, PRESENT, data complexity, success probability, time complexity

**Date:** received 7 Mar 2011, last revised 23 Jun 2011

**Contact author:** celine blondeau at inria fr