Cryptology ePrint Archive: Report 2011/616

Impossible Differential Cryptanalysis of the Lightweight Block Ciphers TEA, XTEA and HIGHT

Jiazhe Chen and Meiqin Wang and Bart Preneel

Abstract: TEA, XTEA and HIGHT are lightweight block ciphers with 64-bit block sizes and 128-bit keys. The round functions of the three ciphers are based on the simple operations XOR, modular addition and shift/rotation. TEA and XTEA are Feistel ciphers with 64 rounds designed by Needham and Wheeler, where XTEA is a successor of TEA, which was proposed by the same authors as an enhanced version of TEA. Whilst HIGHT, which is designed by Hong et al., is a generalized Feistel cipher with 32 rounds and eight 8-bit words in each round. On the one hand, all these ciphers are simple and easy to implement; on the other hand, the diffusion is slow, which allow us to find some impossible properties.

This paper proposes a method to identify the impossible differentials for TEA and XTEA by using the diffusion property of these block ciphers, where the impossible differential comes from one bit contradiction. By means of the method, 14-round impossible differential of XTEA and 13-round impossible differential of TEA are derived, which results in improved impossible differential attacks on 23-round XTEA and 17-round TEA, respectively. These attacks significantly improve the previous 11-round impossible differential attack on TEA and 14-round impossible differential attack on XTEA given by Moon et al. from FSE 2002. For HIGHT, we improve the 26-round impossible differential attack proposed by \"{O}zen et al.; an impossible differential attack on 27-round HIGHT that is slightly faster that the exhaustive search is also given. The attacks on TEA, XTEA and HIGHT are also the best attacks in terms of time complexity.

Category / Keywords: secret-key cryptography /

Date: received 16 Nov 2011, last revised 17 Apr 2012

Contact author: jiazhechen at gmail com