Cryptology ePrint Archive: Report 2013/070

Related-key Attacks Against Full Hummingbird-2

Markku-Juhani O. Saarinen

Abstract: We present attacks on full Hummingbird-2 which are able to recover the 128-bit secret keys of two black box cipher instances that have a certain type of low-weight XOR difference in their keys. We call these highly correlated keys as they produce the same ciphertext with a significant probability. The complexity of our main chosen-IV key-recovery attack is 2^{64}. The first 64 bits of the key can be independently recovered with only 2^{36} effort. This is the first sub-exhaustive attack on the full cipher under two related keys. Our attacks use some novel tricks and techniques which are made possible by Hummingbird-2's unique word-based structure. We have verified the correctness and complexity of our attacks by fully implementing them. We also discuss enabling factors of these attacks and describe an alternative design for the WD16 nonlinear keyed function which is resistant to attacks of this type. The new experimental function replaces S-boxes with simple χ functions.

Category / Keywords: secret-key cryptography / Hummingbird-2, Related-Key Cryptanalysis, Lightweight Cryptography, Authenticated Encryption, Hummingbird-2nu

Publication Info: FSE 2013, March 11-13, 2013, Singapore.

Date: received 14 Feb 2013, last revised 11 Mar 2013

Contact author: mjos at iki fi