Cryptology ePrint Archive: Report 2011/531

Static Fault Attacks on Hardware DES Registers

Philippe Loubet-Moundi and David Vigilant and Francis Olivier

Abstract: In the late nineties, Eli Biham and Adi Shamir published the first paper on Differential Fault Analysis on symmetric key algorithms. More specifically they introduced a fault model where a key bit located in non-volatile memory is forced to $0/1$ with a fault injection. In their scenario the fault was permanent, and could lead the attacker to full key recovery with low complexity. In this paper, another fault model is considered: forcing a key bit to $0/1$ in the register of a hardware block implementing Data Encryption Standard. Due to the specific location of the fault, the key modification is not permanent in the life of the embedded device, and this leads to apply a powerful safe-error like attack. This paper reports a practical validation of the fault model on two actual circuits, and discusses limitations and efficient countermeasures against this threat.

Category / Keywords: Hardware DES, fault attacks, safe-error, register attacks

Date: received 30 Sep 2011, last revised 5 Oct 2011

Contact author: philippe loubet-moundi at gemalto com

Available formats: PDF | BibTeX Citation

Note: Give the exact reference to patent (old reference [16])

Version: 20111005:140737 (All versions of this report)

Discussion forum: Show discussion | Start new discussion