Cryptology ePrint Archive: Report 2011/349

Efficient Methods for Exploiting Faults Induced at AES Middle Rounds

Chong Hee Kim

Abstract: Faults occurred during the operations in a hardware device cause many problems such as performance deterioration, unreliable output, etc. If a fault occurs in a cryptographic hardware device, the effect can be even serious because an adversary may exploit it to find the secret information stored in the device. More precisely, the adversary can find the key of a block cipher using differential information between correct and faulty ciphertexts obtained by inducing faults during the computation of ciphertexts. This kind of attack is called \emph{Differential Fault Analysis} (DFA). Among many ciphers \emph{Advanced Encryption Standard} (AES) has been the main target of DFA due to its popularity. AES is widely used in different platforms and systems including Intel and AMD microprocessors. Normally DFA on AES exploits faults induced at the last few rounds. Hence, a general countermeasure is to recompute the last few rounds of AES and compare it with the original output. As redundancy is a costly countermeasure, one should ascertain exactly which rounds need to be protected. In 2006, Phan and Yen introduced a new type of DFA, so called Square-DFA, that works even when faults are induced into some middle rounds. However, it is impractical as it requires several hundreds of faulty ciphertexts as well as a bit fault model. In this article, we propose new attacks that need only dozens of faulty ciphertexts in a byte fault model. Normally it is believed that randomly corrupting a byte is easier than corrupting a specific bit. In addition, we extend the attacks to the AES-192 and AES-256, which is the first result in the literature.

Category / Keywords: secret-key cryptography / Differential Fault Analysis, AES.

Date: received 27 Jun 2011

Contact author: chhkim7 at gmail com