Waveforms re-alignment to improve DPA attacks

G. Di Natale, M.-L. Flottes, B. Rouzeyre, M.Valka
Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier (LIRMM)
Université Montpellier II / CNRS UMR 5506
Montpellier, France
{dinatale, flottes, rouzeyre, valka}@lirmm.fr

Abstract

In all differential power analysis methods, the basic idea underlying the attack is that the instantaneous amount of energy used by the circuit during an encryption operation depends on the actual values of the manipulated data.
Based on this assumption and by focusing on a part of the circuit that operates on a small part of the cyphertext and the secret key (for instance the output of an Sbox in AES algorithm that depends on 8 bits only), the attacker can guess all the sub-keys. For each of them he/she can determine the correlation between a model of the power consumption for such a key guess and the actual power consumption of the circuit. The best correlation should correspond to the correct secret key.

In this talk we will present how the knowledge of the structure of the circuit can be exploited to improve the DPA attack. We propose to perform a timing simulation of the circuit by guessing all the secret keys. This simulation is used to determine the instant when the energy consumed by the circuit is highly correlated to the secret key. Then DPA is performed by re-aligning the waveforms of the power consumption of the circuit according to the timing values obtained by the timing simulation.
We will present the result of this study on combinational circuits and we will show the effectiveness of the proposed method.