Cryptology ePrint Archive: Report 2011/162

Collision Timing Attack when Breaking 42 AES ASIC Cores

Amir Moradi and Oliver Mischke and Christof Paar

Abstract: A collision timing attack which exploits the data-dependent timing characteristics of combinational circuits is demonstrated. The attack is based on the correlation collision attack presented at CHES 2010, and the timing attributes of combinational circuits when implementing complex functions, e.g., S-boxes, in hardware are exploited by the help of the scheme used in another CHES 2010 paper namely fault sensitivity analysis. Similarly to other side-channel collision attacks, our approach avoids the need for a hypothetical model to recover the secret materials. The results when attacking all 14 AES ASIC cores of the SASEBO LSI chips in three different process technologies, 130nm, 90nm, and 65nm, are presented. Successfully breaking the DPA-protected and the fault attack protected cores indicates the strength of the attack.

Category / Keywords: implementation / Timing Attack, Collision Attack, Fault Sensitivity, AES, ASIC

Date: received 31 Mar 2011, last revised 1 Apr 2011

Contact author: moradi at crypto rub de