Cryptology ePrint Archive: Report 2011/579

Clockwise Collision Analysis -- Overlooked Side-Channel Leakage Inside Your Measurements

Yang Li and Daisuke Nakatsu and Qi Li and Kazuo Ohta and Kazuo Sakiyama

Abstract: This paper presents a new side-channel attack technique called {\it clockwise collision} analysis. For the cryptographic implementations using synchronous digital circuit with a loop architecture, signal transitions as well as the side-channel leakage relates to not only the input data in the current cycle, but also the status in one-cycle before. The clockwise collision utilizes the fact that little computation is required in the second clock cycle when the inputs for two consecutive clock cycles are the same. In contrast, the previously known {\it computational collision} utilizes the fact that the computation of the same input value leads to similar side-channel leakage. By experimentation, we demonstrate the feasibility and vulnerability for this novel clockwise collision analysis both by injecting faults and by analyzing the power consumption.

Category / Keywords: implementation / Side-channel attack, clockwise collision, fault, power consumption

Date: received 26 Oct 2011

Contact author: liyang at ice uec ac jp

Available formats: PDF | BibTeX Citation

Version: 20111102:204201 (All versions of this report)

Discussion forum: Show discussion | Start new discussion