External Awards

IEICE ELEX Best Paper Award in the Year 2012

Winners: Yoshio Takahashi[†1] and Tsutomu Matsumoto[†2]
†1 System Platforms Sector, NTT DATA Corporation
†2 Graduate School of Environment and Information Sciences, Yokohama National University

Date: September 18, 2013

Organization: The Institute of Electronics, Information and Communication Engineers (IEICE)

For "A Proper Security Analysis Method for CMOS Cryptographic Circuits".

Differential Power Analysis (DPA) aims at revealing secret keys in cryptographic devices by analyzing their power consumption as side-channel information. Although power consumption models based on transition probability were used to evaluate DPA resistance in previous studies, the adequacy of these models has not been adequately confirmed. In this paper, we describe two experiments on obtaining precise information of power consumption, and show that Random Switching Logic, one of the DPA countermeasures, is in reality not secure against DPA.

Published as: Y. Takahashi and T. Matsumoto, "A Proper Security Analysis Method for CMOS Cryptographic Circuits," IEICE Electronics Express, Vol. 9, No. 6, pp. 458–463, 2012.