University of Victoria | Graduate Studies

Notice of the Final Oral Examination for the Degree of Doctor of Philosophy

of

ZIYAD ALMOHAIMEED

MSc (University of Victoria, 2013)
BSc (Qassim University, 2009)

“Secured-by-Design FPGA against Side-Channel Attacks Based on Power Consumption”

Department of Electrical and Computer Engineering

Wednesday, July 26, 2017
8:00 A.M.
Engineering and Computer Science Building
Room 468

Supervisory Committee:
Dr. Mihai Sima, Department of Electrical and Computer Engineering, University of Victoria (Supervisor)
Dr. Stephen Neville, Department of Electrical and Computer Engineering, UVic (Member)
Dr. Florin Diacu, Department of Mathematics and Statistics, UVic (Outside Member)

External Examiner:
Dr. Serioja Tatu, Energie Materiaux et Telecommunications, Institut National de la Recherche

Chair of Oral Examination:
Dr. Michel Lefebvre, Department of Physics and Astronomy, UVic

Dr. David Capson, Dean, Faculty of Graduate Studies

Abstract

Power Analysis Attack poses a serious threat to a behavioural implementation of the well-known cryptosystem. The attack exploit the relation between power consumption and the processed data (secret key). Field Programmable Gate Array (FPGA) has emerged as an attractive platform that provide hardware-like performance with software-like flexibility. These features come at the expense of larger power consumption which makes the FPGA very vulnerable to power attacks. Different countermeasures have been introduced in the literature. Such countermeasures have been originally developed for ASICs; thus, mapping them onto FPGA degrades their effectiveness. In this work, we tackled the cause of the problem by proposing a secure-by-design techniques that not only provide robustness to switching power attacks but to all power related attacks namely dynamic, static, glitches, and early evaluation. The reconfigurability of the platform is preserved; thus, the comfort of implementing robust cryptosystems without any special design techniques is offered to cryptosystems developers. The silicon area overhead is in line with prior art.