

Securing Light Weight Cryptographic Implementations on FPGAs Using DPL

A Master's Thesis Presentation.

By

Rajesh Velegalati

Advisor: Dr Jens-Peter Kaps.

**Monday, July 27th 2009 @ 4:00PM
Engineering Building, Room 3507
Department of Electrical and Computer Engineering
George Mason University.**

Abstract

Recent advances in Field Programmable Gate Array (FPGA) technology are bound to make FPGAs a popular platform for battery powered devices. Many applications of such devices are mission critical and require the use of cryptographic algorithms to provide the desired security. However, Differential Power Analysis (DPA) attacks pose a severe threat against otherwise secure cryptographic implementations.

Current techniques to defend against DPA attacks such as Dual rail with Pre-Charge Logic (DPL) lead to an increase in area consumption of factor 4 or more which is not suitable for Light Weight implementations. Current secure implementations using DPL require ASIC tools and a special ASIC library. In this thesis we show that moderate security against DPA attacks can be achieved for DPL secured implementations using only FPGA CAD tools augmented by some scripts. The resulting circuit has an area increase of not much more than a factor two over standard FPGA implementations. We demonstrate our approach by implementing a cryptographic algorithm on Spartan3E FPGA and assessing the security it provides against DPA. We also study one of the Xilinx FPGA specific intrinsic features - Wide Dedicated Multiplexer (WDM) -with respect to DPA.