Implementation Diversity and Dynamic Partial Reconfiguration for Impeding Differential Power Analysis Attacks on FPGAs

Nahome G. Bete, Meghanath Nakka and Jim Plusquellic
ECE, Univ. of New Mexico
Albuquerque, NM

Fareena Saqib
ECE, Florida Institute of Technology
Melbourne, FL

Chintan Patel and Ryan Robucci
CSEE, Univ. of Maryland, Balt. Co.
Baltimore, MD

This hardware demonstration investigates countermeasures to side-channel-based attack mechanisms. In particular, we focus on developing methods that are designed to make differential and correlation power analysis, referred to as DPA and CPA, as well as Electromagnetic analysis (EMA) techniques, ineffective as an attack vector. Our technique leverages dynamic partial reconfiguration capabilities available in modern FPGA-based system-on-chip hardware platforms as a means of introducing uncertainty in the analysis of power supply transient signals. The proposed technique involves rapidly changing the implementation characteristics of components of the encryption algorithm, while preserving the functionality, using DPR methods. We propose to change small components of the circuit implementation, e.g., one or more of the SBOX instantiations of the AES algorithm, rapidly during the operation of the encryption using DRP. A set of different instantiations will be stored within FPGA Block RAM resources (or secure processor side memory) and a DPR Controller state machine running in parallel with the cryptographic primitive will be designed to synchronize with the AES to enable periodic reconfiguration.

1. INTRODUCTION

This hardware demonstration investigates countermeasures to side-channel-based attack mechanisms. In particular, we focus on developing methods that are designed to make differential and correlation power analysis, referred to as DPA and CPA, as well as Electromagnetic analysis (EMA) techniques, ineffective as an attack vector. DPA and CPA are particular problematic because 1) they enable high resolution visibility into the gate-level switching behavior of the chip, 2) they are semi-invasive and non-destructive, requiring only benchtop test and measurement equipment (that are widely available and becoming cost effective), 3) with additional time and processing, they have been shown to be successful despite many of the proposed design-oriented countermeasures.

Our technique leverages dynamic partial reconfiguration capabilities available in modern FPGA-based system-on-chip hardware platforms as a means of introducing uncertainty in the analysis of power supply transient signals. Reconfigurable hardware is increasingly being integrated into microprocessor environments and therefore, the opportunity to leverage DPR is expanding. The proposed technique involves rapidly changing the implementation characteristics of components of encryption algorithm (while preserving the functionality) using DPR methods as a means of violating the fundamental assumption on which DPA depends. DPA derives its power by averaging power transient signals measured from an underlying invariant circuit implementation. We propose to change small components of the circuit implementation, e.g., one or more of the SBOX instantiations of the AES algorithm, rapidly during the operation of the cryptographic primitive using DRP.

A set of different instantiations are stored within FPGA Block RAM resources (or secure processor side memory) and a DPR Controller state machine running in parallel with the encryption engine synchronizes with AES to enable periodic reconfiguration. Implementation diversity techniques are used to introduce small changes in components of the instantiated design. For example, Fig. 1 shows one

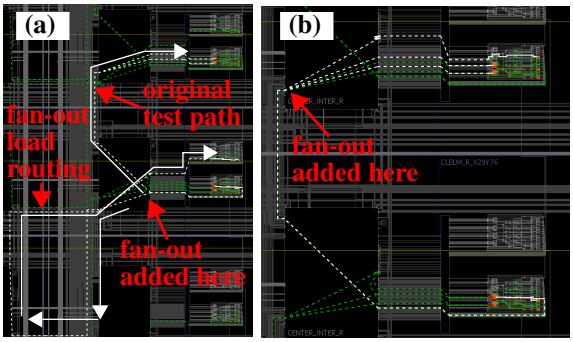

Fig. 1. Implementation diversity introduced manually by introducing small changes in wire routes.

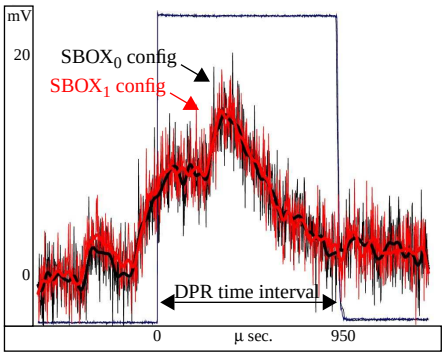

Fig. 2. Power transients from a DPR operation using two slightly modified versions of SBOX.

such technique in which wire routes are modified by hand. The routing changes must be significant enough to change the power transient but small enough to make it impossible for the adversary to determine which of *n* implementations is being programmed. Fig. 2 shows power transients collected during the DPR operation using two slightly different implementations of the AES SBOX component. The objective of our technique is to add 'noise' to the power transients, leaving random artifacts in the averaged power transient waveforms, while minimizing delays and energy consumption.

2. Observables in Hardware Demonstration

A Xilinx Zynq FPGA SoC will be used as the test platform in the hardware demonstration. A controller state machine, implemented in VHDL, will randomly select and re-program portions of a fully operational and functioning AES engine once every millisecond using the TRNG data of a physical unclonable function. The partial programming bitstrings will be loaded into PL-side BRAM from a trusted execution environment (TEE) running under Linux using Xilinx TrustZone. An oscilloscope will be used to measure power transient waveforms and a software version of the DPA algorithm will be used to average and correlate them to determine if peaks normally present without the countermeasure reduce or disappear when the countermeasure is enabled.