EasyChair Preprint

№ 788

A 128-bit AES Engine with Higher Resistance to Power & Electromagnetic Side-Channel Attacks Enabled by a Security-Aware Integrated All-Digital Low Dropout Regulator

Arvind Singh, Monodeep Kar, Sanu Mathew, Anand Rajan, Vivek De and Saibal Mukhopadhyay

February 22, 2019

A 128-bit AES Engine with Higher Resistance to Power & Electromagnetic Side-Channel Attacks Enabled by a Security-Aware Integrated All-Digital Low Dropout Regulator

[1]A. Singh, [2]M. Kar, [2]S. Mathew, [2]A. Rajan, [2]V. De, [1]S. Mukhopadhyay
[1]Georgia Institute of Technology, Atlanta, GA; [2]Intel, Hillsboro, OR

1 Hardware Demo Objectives

*In the demonstration session, we will be presenting a test-chip and the PCB designed to measure the side channel activity for digital low dropout (DLDO) regulator-based side channel analysis attack countermeasures (**the paper based on the same test-chip was presented at IEEE International Solid-State Circuits Conference (ISSCC), in February 2019 [1] along with the hardware demonstration presentation**).*

2 Introduction

Recently, there has been many works which have developed side channel countermeasures exploiting on-chip integrated power management modules and have validated the improvement in side channel resistance with experimental analysis [2-5]. These countermeasures employ inductive voltage regulator which are complex in nature and require large passives to be integrated on-chip. This demonstration presents an on-chip integrated all-digital low-dropout (DLDO) regulator based countermeasures for encryption engines against side channel analysis (SCA) attacks. DLDOs are increasingly integrated with modern SoC systems for ultra fine-grained power management and point of load regulation. This demonstration for the first time leverages DLDOs along with some additional circuit techniques to enhance SCA resistance of advanced encryption standard (AES) engines and presents experimental results and analysis. Our poster will show the motivation behind the proposed work, overall architecture and details about measurement setup, analysis techniques and side channel attack results with CPA/CEMA for two different architectures of advanced encryption standard (AES) engines – parallel AES (P-AES) and serial AES (S-AES).

3 Attack Model

We will demonstrate acquisition of both power (with SMA based voltage probes) and EM signatures with beehive EMC probes (small loop area – 0.4" and high bandwidth – 1GHz Picoscope which samples the analog/digital signals and transfers to PC for display will be used for displaying these signatures. We will demonstrate power/EM signatures under individual SCA improvement schemes (standalone AES, DLDO-AES system, and DLDO-AES system with proposed randomization circuits, namely switching noise injector - SNI and Random VREF generation - R-VREF). Two different architectures for advanced encryption standard (AES), namely parallel and serial along with bit-serial architecture SIMON will be demonstrated in conjunction with DLDO based countermeasures. Correlation power analysis (CPA) in frequency domain with pre-processing techniques (filtering) will be demonstrated as key recovery attacks and test-vector leakage assessment (TVLA) will be presented as leakage detection methodology.

4 Experimental Results

We will show how the signatures vary for parallel-AES (P-AES) and serial-AES (S-AES) due to different amount of instantaneous current drawn by these cores. We plan to show TVLA analysis and CPA/CEMA on real-time acquisitions of signatures for standalone AES. However, due to large number of measurements required for DLDO-AES, the TVLA and CPA/CEMA analysis will be shown on already acquired/saved signatures. We will use python based setup to analyze these signatures and display them in a UNIX-based GUI. In case there is any problem with PCB/test-chip being non-functional during the demo session, we will prepare a video describing the measurement setup and signature acquisition in our lab environment and explain rest of the results with poster.

5 Key Observations and Outcomes

DLDO-based countermeasures are able to increase the SCA resistance of AES engines by upto 3579X at very small design area/power increase and only 10% performance overhead.

6 List of Equipment

Required equipment that we will be bring with us are listed here: 1) Test PCB with the test-chip, 2) Picoscope for signal acquisition, 3) Personal computer for processing, 4) Power supplies – through USB cables supplying

current to multiple on-board voltage regulator modules, 4) Monitor to display the waveforms and analysis results.

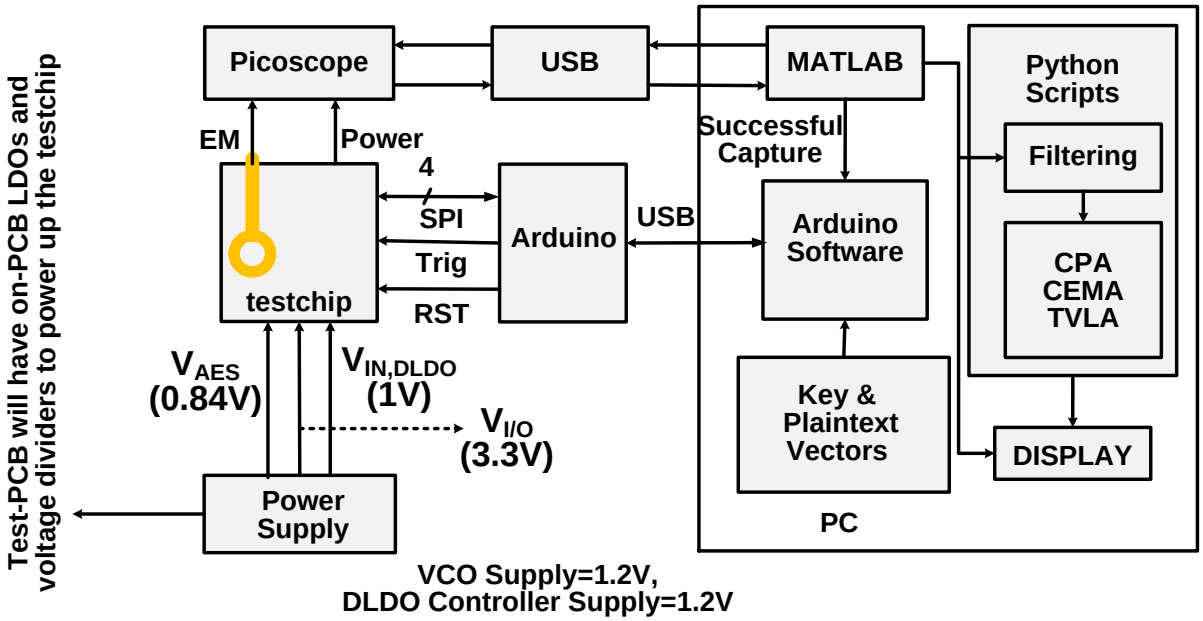

Figure 1. The block diagram shows the measurement setup for side channel acquisition and analysis in detail.

7 References

[1] A. Singh, M. Kar, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "A 128-bit AES Engine with Higher Resistance to Power & Electromagnetic Side-Channel Attacks Enabled by a Security-Aware Integrated All-Digital Low Dropout Regulator," accepted for publications in International Solid-State Circuits Conference (ISSCC), 2019.

[2] M. Kar, A. Singh, S. K. Mathew, A. Rajan, V. De and S. Mukhopadhyay, "Reducing Power Side-Channel Information Leakage of AES Engines Using Fully Integrated Inductive Voltage Regulator," in IEEE Journal of Solid-State Circuits, vol. 53, no. 8, pp. 2399-2414, Aug. 2018.

[3] M. Kar, A. Singh, S. Mathew, A. Rajan, V. De and S. Mukhopadhyay, "8.1 Improved power-side-channel-attack resistance of an AES-128 core via a security-aware integrated buck voltage regulator," 2017 IEEE International Solid-State Circuits Conference (ISSCC), San Francisco, CA, 2017, pp. 142-143.

[4] A. Singh, M. Kar, S. K. Mathew, A. Rajan, V. De and S. Mukhopadhyay, "Improved Power/EM Side-Channel Attack Resistance of 128-Bit AES Engines With Random Fast Voltage Dithering," in IEEE Journal of Solid-State Circuits.

[5] A. Singh, M. Kar, S. Mathew, A. Rajan, V. De and S. Mukhopadhyay, "Improved power side channel attack resistance of a 128-bit AES engine with random fast voltage dithering," ESSCIRC 2017 - 43rd IEEE European Solid State Circuits Conference, Leuven, 2017, pp. 51-54.