Poster: Hardware and Software Emission Analysis

Dmitry Nedospasov*, Jean-Pierre Seifert
Security in Telecommunications,
Dept. of Software Engineering and Theoretical Computer Science,
Technische Universität Berlin,
Berlin, Germany
{dmitry,jpseifert}@sec.t-labs.tu-berlin.de

Alexander Schlösser*, Susanna Orlic
Optical Technologies,
Institute for Optics and Atomic Physics,
Technische Universität Berlin,
Berlin, Germany
{schloesser,orlic}@opttech.tu-berlin.de

* These authors contributed equally to this work

I. Introduction

The legacy nature of many of today's secure integrated circuits (ICs) means that attackers have been able to hone their attacks as the target platform is continuously refined. Increasing complexity as well obfuscation in a layered defense strategy has allowed many manufacturers to protect designs from threats such as IP theft. Vendors continue to shrink feature sizes, design and synthesize logic in non-standard styles and add additional layers of obfuscation, such as memory and bus encryption and current-carrying interconnects, commonly referred to as active meshes [3]. Prior to attacking a secure IC an attacker must identify the parts of the layout and their function, yet, this is becoming an increasingly difficult and costly process for the attacker.

In this work we demonstrate an efficient, fully-automated, low-cost method for performing functional analysis of a given IC by analyzing the photonic emissions produced by code executed on the chip. Since our methodology employs semi-invasive backside analysis, it is not impeded by industry-standard countermeasures such as active meshes.

In this work we:

- Develop a software generation framework for automated IC analysis.
- Develop an inexpensive setup for efficient, automated backside optical functional analysis of ICs.
- Identify specific functional groups of an IC.
- Identify the code being executed on the IC based on the emissions.
- Provide practical results for a common, commercially available microcontroller, the ATmega328P.

It is important to consider how our methodology compares to other techniques for IC analysis. Picosecond Imaging Circuit Analysis (PICA) is based on infrared-sensitive gated multi channel plates and provides both temporal and spatial resolution. One of the first works to PICA in a security application was [2], where PICA is utilized to attack the `AddRoundKey` operation of AES [1]. In [6] the authors use PICA to develop methods for detecting malicious additions to an IC. However, the cost and complexity of PICA equipment makes it a non-viable choice in real world attacks.

The idea of using a low-cost Si-CCD capable of recovering the photonic emissions from the silicon substrate via backside analysis, was introduced in [4], [5]. These works also note the potential for applying such methodologies to reverse-engineer ICs. Our methodology also employs a low-cost Si-CCD to recover emissions via backside analysis. In contrast to [5], instead of using a laser to identify interesting areas of a chip, we developed a methodology based on selectively executing code on the chip. By creating loops that are short in length we can maximize the emissions of certain parts of the chip and thus identify their function. This can eliminate the tedious exhaustive search that is the basis of many attacks. By studying the optical emissions it is possible to directly identify potential target areas of the chip.

II. Hardware

The hardware setup consists of a Si-CCD camera directly connected to interchangeable microscope objectives and two perpendicularly arranged linear stages onto which a custom printed circuit board (PCB) is mounted with the device under test (DUT).

The optic's design has been kept to an absolute minimum to maximize system throughput and analysis efficiency. We use finite-conjugate reflection type objectives with gold plated mirrors. This way 85% of the captured light reaches the camera; Absorption of NIR photons, common in glass objectives and tube lenses is bypassed. We also use a special CCD sensor type that has become usable for scientific applications in recent years. Back illuminated deep depletion sensors feature the highest NIR quantum efficiency in silicon detectors yet. At 900nm, over 90% of the impeding photons are detected. To avoid dark current and readout noise the sensor and preamp are thermoelectrically cooled to -70°C and shift and readout rates are customizable.

The DUT is placed into a cavity in the middle of the PCB and soldered upside down. For our experiments, the PCB consisted of the ATmega328p, which was provided an external 16MHz clock from a standard quartz oscillator on the PCB, and a connection to the measurement PC. In addition to an increased software loop frequency, substrate thinning can greatly improve the acquisition time.

A. Software

To efficiently test input sets of several hundred subroutines the chip must be programmed in such a way that it executes a new subroutine on every boot. Thus, the code generation framework must implement the following features: (1) In order to keep track, the state must be saved to non-volatile memory. Specifically in our implementation, an integer is saved to the chip's EEPROM and is incremented at every boot. (2) Since the amount of subroutines is of variable length, the control code must also be generated automatically. Our implementation generated wrapper files written in C containing a switch-case that receives the integer from EEPROM as input and calls a different subroutine based on the value of the integer. (3) Finally, the subroutines themselves must also be automatically generated. Our framework generates an assembly file that contains the entire set of subroutines to be executed by the chip.

By passing multiple arguments to the framework a test set of arbitrary size can be specified. The scripts generate all the necessary wrapper files and subroutines. Thus, the chip can easily be programmed with a workload of several hundred test cases and left to run autonomously with no additional user input. The measurement PC resets the chip (causing it to execute the next subroutine), triggers the camera to take an image, saves the image and repeats the process until images are taken for the entire test set.

III. Results

Using this methodology we were able to achieve several important practical results.

1) Eliminating large areas of the IC: By creating a set of reference images it is possible to quickly identify parts of the IC are logic. More importantly, this process eliminates large ares of the chip that are not of particular interest, such as voltage and clock distribution circuits and sense amplifiers of memories.

Using optical emissions we were able to identify the physical location of each address within the SRAM. Moreover, we were able identify the byte order of each line of SRAM, yielding the physical location of each bit within memory.

2) Identifying branching logic: By computing the difference images of operations on the `avr`-architecture's status registers we were able to identify unique emissions for each status bit. The optical emissions could then be clearly identified in the emission images of conditional branching operations that operated on these status registers.

3) Identifying execution logic: By executing identical code at different addresses we were able to identify address-dependant logic. Specifically we identified the circuitry responsible for addressing program memory.

4) Identifying the executed code: Given the memory layout, the physical position of the stack can be easily identified. Commonly used variables within memory can also stand out in the emissions. The contrast within the emission images also reflects access patterns to different parts of the chip. The length of the code segment being executed, for example, can be estimated by observing the control logic of the program memory.

References

[1] W. Rankl and W. Effing, *Smart Card Handbook*, fourth edition ed. Wiley, 2010.

[2] J. Ferrigno and M. Hlaváč, "When AES blinks: introducing optical side channel," *IET Information Security*, vol. 2, no. 3, p. 94, 2008.

[3] "Advanced Encryption Standard (AES)," Nov. 2001.

[4] P. Song, F. Stellari, D. Pfeiffer, J. Culp, A. Weger, A. Bonnoit, B. Wisnieff, and M. Taubenblatt, "MARVEL — Malicious alteration recognition and verification by emission of light," *Hardware-Oriented Security and Trust (HOST), 2011 IEEE International Symposium on*, pp. 117–121, 2011.

[5] S. Skorobogatov, "Using Optical Emission Analysis for Estimating Contribution to Power Analysis," *Fault Diagnosis and Tolerance in Cryptography, FDTC 2009*, pp. 111–119, 2009.

[6] ——, "Optical Fault Masking Attacks," *Fault Diagnosis and Tolerance in Cryptography, FDTC 2010*, pp. 23–29, 2010.