# Power-Based Side-Channel Attack for AES Key Extraction on a ATMega328 controller

Utsav Banerjee, Lisa Ho, and Skanda Koppula

***Abstract*—We demonstrate extraction of a private-key from Flash program memory on the ATMega328 microcontroller (the controller used on the popular Arduino Uno/Genuino board). We loaded a standard AVR-architecture AES implementation onto the chip and ran this implementation to encrypt 500 randomly chosen plaintexts. By carefully measuring the chips power consumption, we were able to correlate the consumed power with the input plaintexts and key values that might be used to encrypt each AES block, and back-derive the hard-coded key used for encryption. We describe here our test infrastructure for automated power trace collection, an overview of our correlation attack, sanitization of the traces and interesting stumbling blocks encountered during data collection and analysis, and the results of our attack.**

***Index Terms*—AES, side-channel, power consumption, ATMega328, Correlation Power Analysis**

## I. Introduction

## II. Preliminaries

### A. Controller Specifications

### B. Correlation Power Analysis

## III. Protocols and Procedure

### A. Data Collection Infrastructure

-

- Discuss trigger with memoery mapped register with assembly sbi instruction, schematic for collection, oscilloscope model/programmer model GPIB with assembly sbi instruction
- Faraday shield metal box
- fast frames

### B. Implementation of CPA and Power Model

- discuss different power models we've tried, faster correlation

### C. Instructive Problems Encountered (and Panaceas)

-

- remove difAmp -¿ increase resistor value -¿ increase bandwidth?//used to measure current before
- serial print adds noise
- averaging to solve dc shift
- interrupt introduces clock jitter
- adding nops to prevent asyncronous / delay
- original hypothesis about sbox: SBox bad for correlation? the flash architecture -¿ bit block bit block bar
- FUNDAMENTALLY A PROBLEM WITH DATA

### D. Overview of Source Code

- overview everything in dropbox

## IV. Results

- go over the graphs, and timing/accuracy results of tests

All authors are with the Department of Electrical and Computer Engineering, Massachusetts Institute of Technology, Cambridge, MA, 02139 USA

To contact the authors: utsav@mit.edu, lisaho@mit.edu, and skandak@mit.edu

Manuscript completed for 6.858 Computer Systems Security; completed on December 5, 2015

## Acknowledgment

The authors would like to extend our deepest thanks to Chiraag Juvekar for the time he spent with us aiding our debugging of data collection and analysis problems.

## References

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.