Conference Paper Title

Zachary Driskill, Jacob Brown, and Jeffrey Goeders
Brigham Young University
450 Engineering Building
Provo, UT 84602
{zd227, jacobb00, jgoeders}@byu.edu

***Abstract*—We did a timing attack.**
***Index Terms*—timing attack, FPGA**

I. Introduction

Timing attacks are a type of side-channel attack.

To further learn about timing attacks, we implemented two simple attacks that exploit a non-constant compare function to extract a secret key.

Our source of inspiration is Joe Grand, who demonstrated a simple timing attack [1].

II. FPGA to MCU

III. Human to FPGA

The purpose of the human-to-FPGA timing attack is to see if it's possible to carry out a toy timing attack using a human and FPGA. The non-constant compare function is implemented on an FPGA and we manually use an oscilloscope to measure time for each compare.

IV. Conclusion

Acknowledgment

Dr. Goeders taught us everything we know about hardware security.

References

[1] Joe Grand. Side channel timing attack demonstration, 2017.