Side Channel Power Analysis of an Embedded Device Running DES

Justin Cox and Tyler Travis
Department of Electrical and Computer Engineering
Utah State University
Logan, Utah 84322
email: justin.n.cox@gmail.com, tyler.travis@aggiemail.usu.edu

***Abstract*— Hardware security is an ever increasing area of study since exploits have been found on computer systems. Encryption algorithms are very difficult to break. Instead of breaking the encryption algorithm, it is common for an attacker to attempt to recover the encryption key instead. One way of recovering the key is using side channel analysis . This paper will discuss a side channel analysis performed on a microcontroller that is operating as a crypto device. The power traces collected will then be analyzed using Differential Power Analysis (DPA) and the results will be shown and discussed.**

***Index Terms*—encryption, decryption, security, DPA, side channel.**

I. INTRODUCTION

Through side channel analysis, an attacker is able to leak information about a device through natural or physical means. In regards to a device running a crypto algorithm, side channel analysis can be used to leak the encryption key. There a many different kinds of side channel attacks, but this paper will focus on obtaining information from the power consumed by the target device. Different operations and data bits require different amounts of power consumption. By recording and analyzing the power consumption, it is possible to obtain the encryption key. The encryption algorithm used in this paper is the Data Encryption Standard (DES).

A DES algorithm will be programmed and uploaded onto a TI Tiva C microcontroller. The algorithm will be ran for many different plaintext inputs and the power consumption will be recorded using an oscilloscope. The power traces will then be analyzed and it will be determined whether or not the secret encryption key can be obtained.

II. DES

A. Overview and Implementation

The type of encryption programmed on the microcontroller will be DES. Although DES is not the current encryption standard and is not as secure as the Advanced Encryption Standard AES, DES is still used in devices today and side channel analysis of a DES crypto device is a valid security risk.

A brief overview of DES will be given so that the reader has a better understanding of how the algorithm works and will better understand where DPA can be used. If the reader would like an in-depth understanding of DES, it is recommended that the reader look to other sources.

The DES algorithm takes a 64-bit plaintext input. It is then run through an initial permutation that outputs 56-bits which are then split into two halves. The data goes through sixteen rounds that each have a sub-key that is generated for each round based on the original 64-bit DES key. After the sixteenth round, the output is run through a finial permutation and the algorithm outputs a 64-bit encrypted ciphertext. The rounds are illustrated in Figure 1.

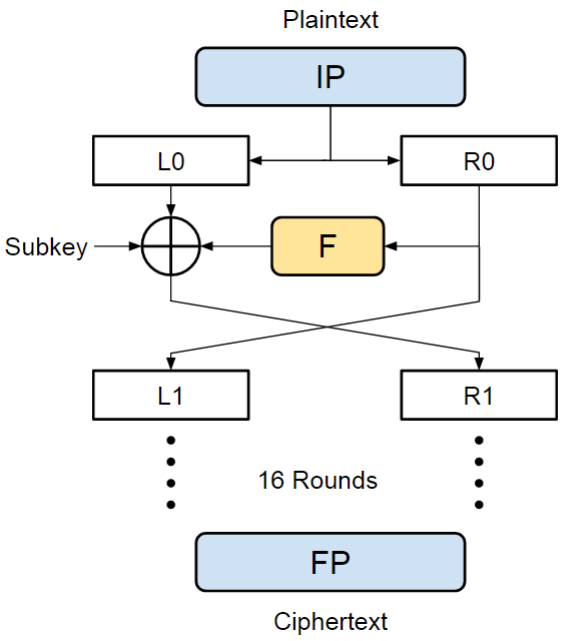

Fig. 1. An illustration of the sixteen round DES algorithm.

During each round, the left 32-bit halve is XORed with the sub key corresponding to the current round as well as the output of the F-function. The inside functionality of the F-function is illustrated in Figure 2. The output of the XOR is used as the next round's right halve and the next round's left halve is the previous round's right halve.

B. Modifications

There were a few minor changes made to the DES algorithm to facilitate the capturing of power traces. These changes do not decrease the security of the DES algorithm. The following assembly routine was added during the last round of the DES algorithm:

```
MOVS   r2,#0x00 ;Set r2 = 0
LDR    r5,[pc,#1012] ;Lower GPIO PIN
LDR    r5,[r5,#0x00]
```

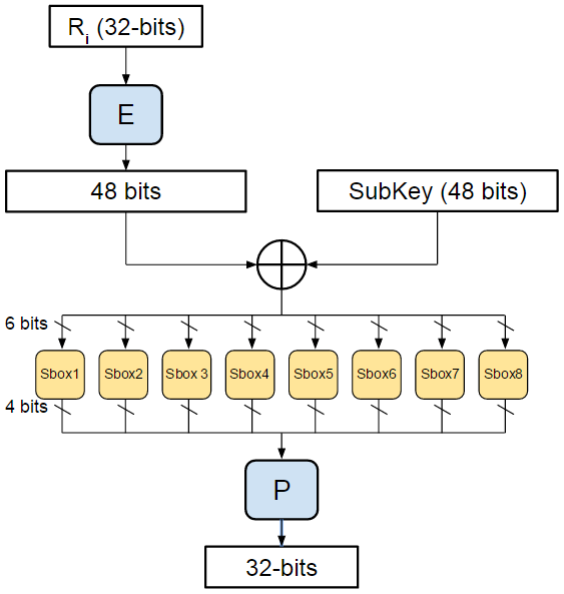

Fig. 2. An illustration of the F-function.

```
BIC     r5,r5,#0x10
LDR     r6,[pc,#1008]
STR     r5,[r6,#0x3FC]

NOP
NOP
NOP
NOP

EOR     r2,r4,r3 ;<--Instruction of Interest

LDR     r5,[pc,#992] ;Set GPIO Pin High
LDR     r5,[r5,#0x3FC]
ORR     r5,r5,#0x10
LDR     r6,[pc,#984]
STR     r5,[r6,#0x3FC]

NOP
NOP
NOP
NOP
```

A GPIO pin on the microcontroller is transitioned from a high to a low in order to trigger the oscilloscope to capture the XOR operation that works with the bits of interest for the DPA. The register that holds the value of the XOR is explicitly set to 0x00 in order to make it easier to measure the Hamming Weight and Distance of that register. This information is helpful for a Correlation Power Analysis (CPA).

III. EXPERIMENTAL SETUP

IV. POWER TRACE ANALYSIS

V. RESULTS

VI. CONCLUSION

REFERENCES

[1] G. Edward Suh, C. W. O'Donnel, I. Sachdev, and S Devadas. Design and Implementation of the AEGIS Single-Chip Secure Processor Using Physical Random Functions. *Proceedings of the 32nd annual international symposium on Computer Architecture*, 2005.

[2] M. Deutschman, "Cryptographic Applications with Physically Unclonable Functions," M.S. Thesis, Inst. Mathematics, Alpen-Adria-Universität Klagenfurt, Klagenfurt, Austria, 2010.

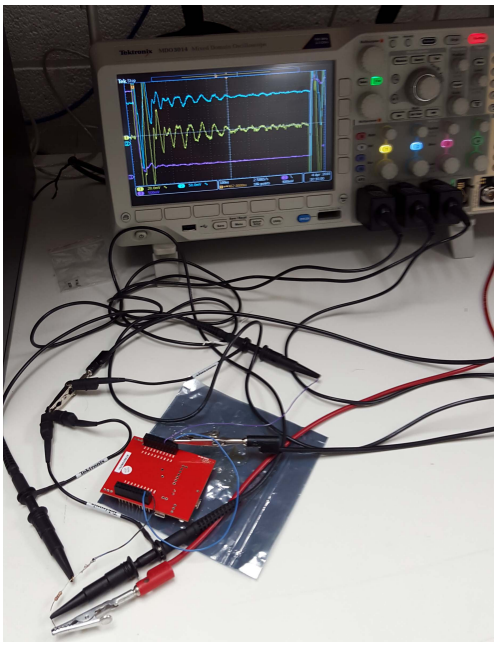

Fig. 3. A picture taken of the experimental setup used.