Utah State University

ECE 5760 Hardware Security

Side-Channel Analysis

John Call, Braydn Clark, Josh Lynn

April 12, 2017

Abstract

Side-Channel Analysis is the process of obtaining information from the physical implementation of a system. This type of analysis can utilize timing information, power consumption, electromagnetism, or other physical characteristics. This paper will focus on side channel analysis of the power consumption of a data encryption standard (DES) algorithm. It will first briefly describe DES and why it is subject to side channel analysis. Second it will describe the method of side channel analysis used, and finally optimizations and other options that could be used.

1 Data Encryption Standard (DES)

Data Encryption Standard is a block cypher, it takes as input a block of plaintext and produces a block of the same size of cyphertext. The algorithm uses a private key to secure the data and prevent the reversal of the encryption. The plaintext block is 64 bits, and it nominally uses a key of the same length, however eight of the bits are not used for the actual encryption making the effective length of the key 56 bits. The 56 bits of the key are modified by a key schedule producing 16 separate subkeys.The subkeys are used to modify the message in 16 rounds that also permute the message. This produces the final cypher text.

1.1 Key Schedule

DES uses a key schedule that produces subkeys for each round of the algorithm. The first step is to apply a permutation that removes 8-bits leaving a 56 bit key divided in two halves. Each half is rotated left by one or two bits depending on the current round. The two rotated halves are passed to the next round and permuted to create a 48 bit round key.

2 Differential Power Analysis

References

[1] M. Aigner and E. Oswald, "Power analysis tutorial," Institute for Applied Information Processing and Communication, Graz, Austria.

[2] J. Li, W. Shan, C.Tian, "Hamming Distance Model Based Power Analysis for Cryptographic Algorithms," National ASIC Center, Southeast University Nanjing, China, October 2011.