Hacking AES
Timothy Chong, Kostis Kaffes
Stanford University
Email: {ctimothy, kkaffes}@stanford.edu

Problem Overview

AES[1] is an encryption specification used in a large variety of applications from encrypting classified documents in government agencies to allowing secure data transfer to everyday transfer protocols, such as HTTPS and FTPS.

In this work, we explore machine learning techniques towards side channel analysis using power-trace to recover AES-128 keys. These techniques include multinomial Gaussian distribution modeling[3] and Support Vector Machine[4].

Support Vector Machine

Balancing skewed hamming weight distribution:
The hamming weights of our data sets are not equally distributed because there is an inherent skewing with the hamming distribution for binary numbers given a set length. To address this, we assign weights inversely proportional to class frequencies in the input data.

Conclusion and Future work

Our work shows it is not a trivial task to predict the hamming weight using a single attack trace. It is worth noting that the inherent skewing of the hamming weight distribution makes it harder to sustain high accuracy while taking into account low frequency hamming weights. The one-bit prediction could alleviate this problem because it does not have to deal with hamming weights.

Several possible improvements include:
- Attack phase isolation on power trace.
- Using Random Forest and/or Neural networks to improve prediction accuracy

Templates Attack

Fig. 3. Template attack flow

Point of interest selection:
Method 1: Find points whose power values vary the most across hamming weight group pairs.
Method 2: Points with highest correlation coefficient between power values and hamming weight.

Experimental Results

Fig. 5. Accuracy of each method with different numbers of POI's and PCA components.

Fig. 6. Precision rate of each hamming weight category.

Fig. 7. Accuracy of a classifier for the first bit of the output of the first phase.

References