Internship Report for CPA on a STM32 Microcontroller

Yufei Wang

University of Illinois at Urbana-Champaign

**Introduction**

The Advanced Encryption Standard(AES) is a widely used encryption method for electronic data. The block size of AES is 128 bits, and the three different key lengths are 128, 192, and 256 bits. The encryption with 128 bits key includes 10 rounds of transformation. All the 10 rounds have steps of SubBytes, ShiftRows, and AddRoundKey, and the first 9 rounds have an extra step called MixColumns. Each round of encryption uses a unique 128 bits round key, which is generated from the initial key. So knowing any of the round key will lead to the recovery of the initial key. It is known that the microcontroller consumes power when it changes a bit of 0 to 1 or from 1 to 0. So there exists a correlation between the number of bits of the encrypted text being changed in each round and the power consumption. A possible round key byte ranges from 0 to 255, therefore, by trying all the possible keys and comparing their correlations with the power usage, the actual key with the strongest correlation will be found. This idea is called Correlative Power Attack(CPA).

**Attack Algorithm**

Although getting any round’s key will lead to the recovery of all the rest keys, the CPA mainly focuses on the last round because it doesn’t have the MixColumns operation, which makes the attack on this round will be easier than the other rounds. Both the hamming distance model and the hamming weight model can represent the number of bits changed during the encryption. For the hamming distance model, each byte of the ciphertext will first XOR with the each of the guessed keys. The XORed bytes will then be substituted by the corresponding subbytes from the inverse S-box. The next step is to find the hamming distance between the subbytes and the original ciphertext. Because of the ShiftRows step, the row index of the corresponding ciphertext is changed. After finding the hamming distances for all 256 key guesses, the final step is to calculate their Pearson's correlation coefficient with the power consumption data. The actual key byte will be the one with the strongest negative correlation. For the hamming weight model, the hamming weight of the subbytes after XOR and inverse S-box substitution will be used for calculating the correlation.

**Experimental Setup**

The board being attacked in the experiment is the STM32F103C8T6 microcontroller. An AES program is uploaded into it via Arduino IDE, and serial communication is enabled to send plaintext and receive ciphertext. The pin A3 of the board is set as the trigger, which will be raised high before the AES started, and set low after the encryption finished. To measure the power consumption of the board, it is connected to a Lecroy WaveRunner 640Zi oscilloscope. 图片包含 室内, 餐桌, 墙壁, 电子产品

描述已自动生成

Collecting Power Trace

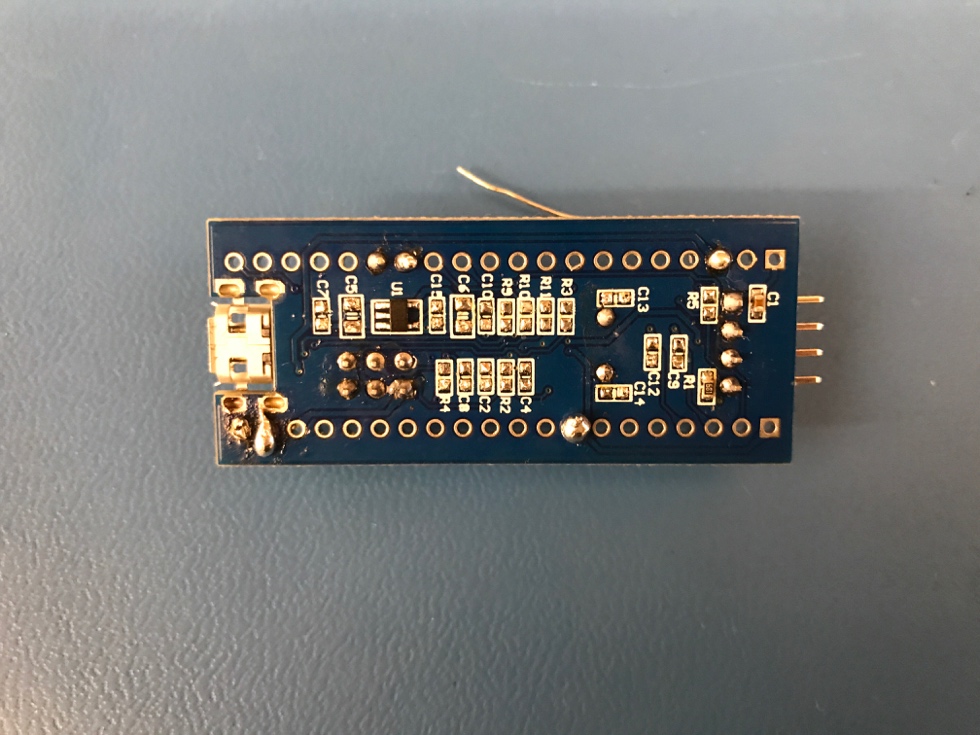
The channel 1 of the oscilloscope connects to the 5V pin of the board with a 1Ω resistor and measures the power consumption. The trigger is connected to channel 2, and the computer provides 5V power to the board through USB. Each power trace collected includes 25,000 sample points. The measuring process is controlled by a python program, which keeps sending randomly generated 16-byte-long plaintexts to the microcontroller and record the ciphertexts. The power data is stored as a binary file which must be transformed into integer by another MATLAB program for CPA attack.

**Preliminary Result**

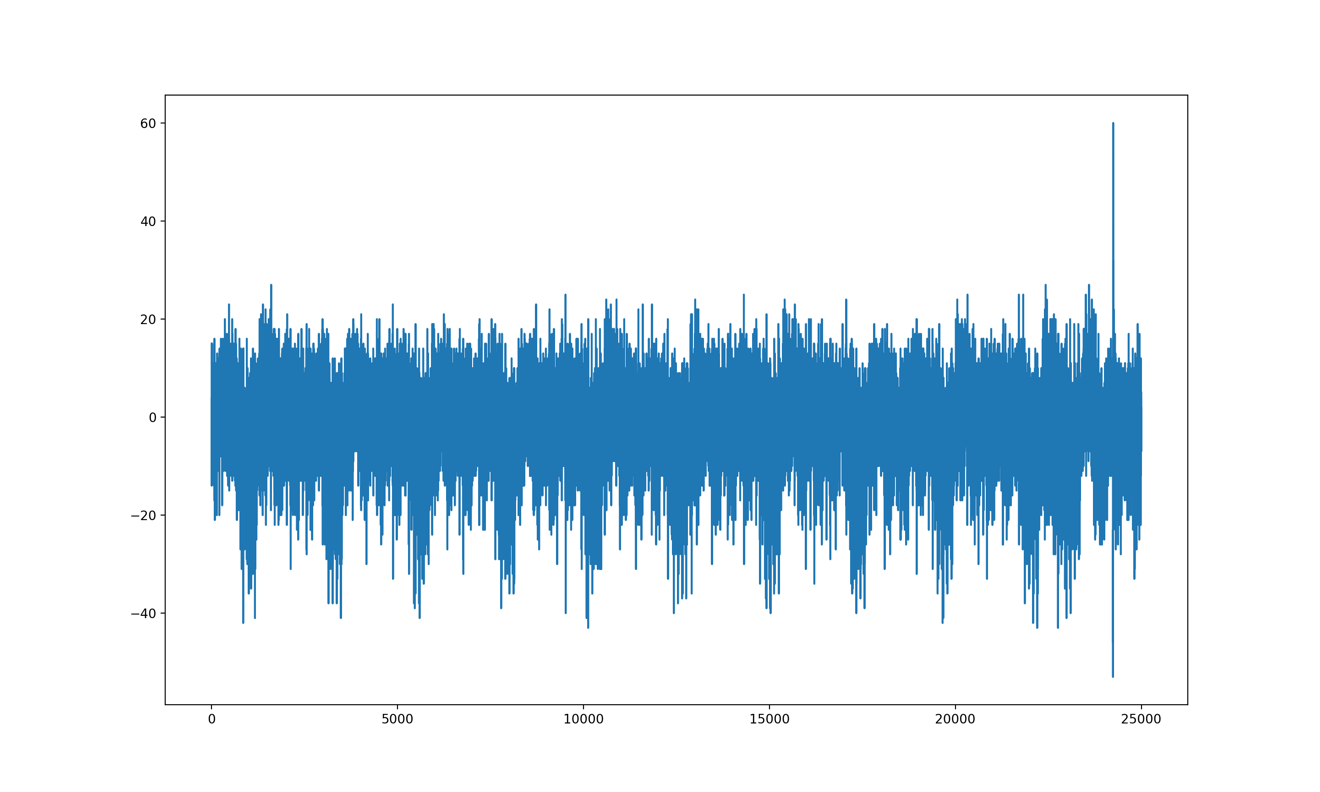
Initially, finding the leakage point is difficult, because the power trace has too much noise which covered all the encryption traces. As the picture reveals, all the 10 rounds of encryption process is covered by noise, so it’s impossible to find the exact location of the last round and attack. To reduce the noise generated by the board, all the capacitors on the back of the board are removed. Because while the AES program is processing, the capacitors keep charging and discharging, which stabilize the current flow in the board and produce a uniform power trace. 图片包含 橱柜, 墙壁, 厨房, 室内

描述已自动生成

Initial Power Trace



Board after Removal of Capacitors

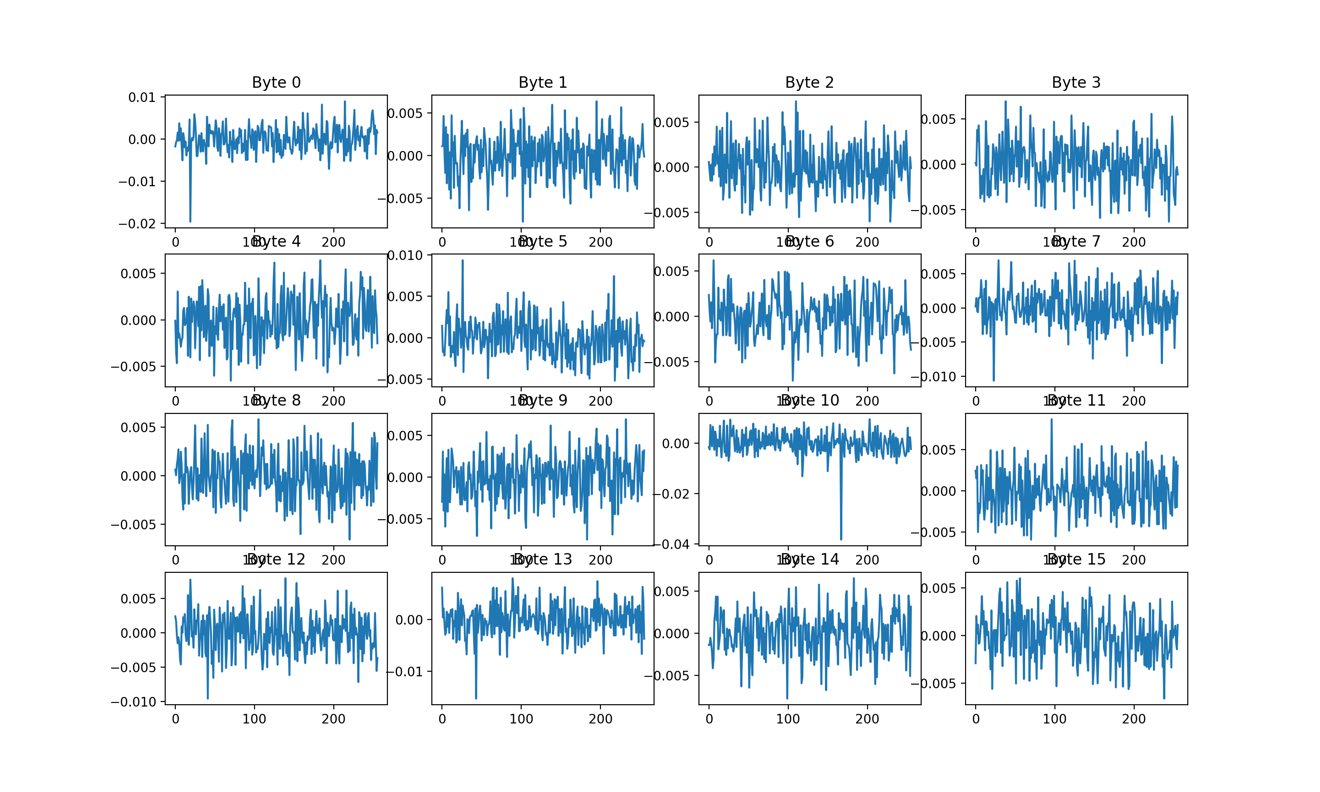


Power Trace after Removal of Capacitors

After the removal of all the capacitors, the power trace becomes cleaner and each round of encryption is now easy to distinguish, the 10th trough is found to be the 10th round of encryption. Leakage points are found in this range for CPA.

**Attack Result**

150,000 power traces were collected for attack. Since storing all these data into one csv file will occupy too much storage, only ten time points on the last round are selected and extracted for analysis. The attack program written in Python reads both the ciphertext and the power trace into lists, and it uses hamming weight model for attack. For each of the 16 bytes round key, the 256 key guesses are divided into several threads using multiprocessing. On a MacBook pro with 4-core CPU, the 256 key guesses are divided into 8 processes for each byte. Part of the result is shown below.



Attack Result

图片包含 电视

描述已自动生成

The initial key is set to be “ 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15”, and the 10th round key should be “19 17 29 127 227 148 74 23 243 7 167 139 77 43 48 197 ”. Unlike attacking FPGA board, which all the 16 bytes key can be recovered using one leakage point, attack on the microcontroller needs several time points to get all the results, because the board encrypts the 16 bytes text one after another, instead of at the same time.

**Conclusion**

In the experiment, the correlative power attack on the STM32 microcontroller is testified. The board is first loaded with an AES program, and the serial communication is enabled. The board is then connected to a oscilloscope to collect power traces while doing encryption. The CPA program is built on the hamming weight model, and 150,000 power traces are utilized to successfully recover the 16 bytes 10th round key. A possible way of countermeasure to this kind of attack is introducing more noise when the board is running. Similar to the idea of removing capacitors to reduce noise, setting extra components on the board to work while the AES is running can cause more power consumption, thus masks the power trace of each round of encryption, and makes it difficult to find the leakage points.