NANYANG TECHNOLOGICAL UNIVERSITY
SINGAPORE

CZ4055: Cyber Physical System Security

Lab 1+2 Report

Sharma Shantanu
U1622895F

Lab Group: CS4

1. Introduction

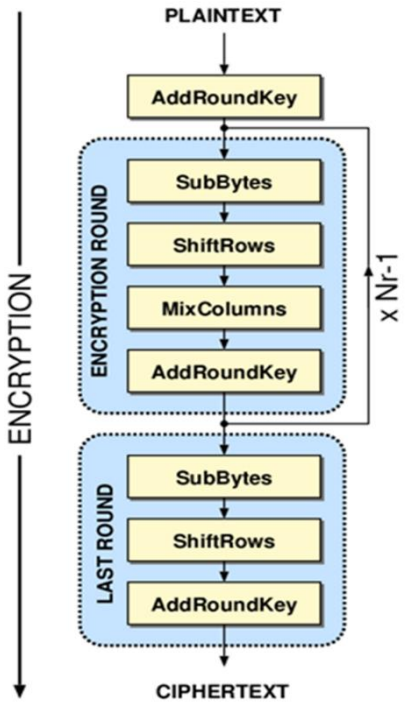
AES is a block cipher initially used by US government and now used worldwide. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. AES is based on a design principle known as a substitution–permutation network and is efficient in both software and hardware. 128-bit version is used extensively where power consumption and/or latency is an issue. Cracking AES-128 key through brute force attack will require computation time billion of times the age of the universe even by the fastest supercomputer. In these two labs we foresaw practical implementation of power-side channel attack on the cryptographic algorithm of AES.

2. Brief Background

2.1 High Level Description of AES-128 algorithm

AES is culmination of multiple Substitution, Shift, and Linear transformation of plaintext to generate ciphertext:

- KeyExpansion
- AddRoundKey
- 9 (typically) Rounds of
  - SubBytes
  - ShiftRows
  - MixColumns
  - AddRoundKey
- Final Round of
  - SubBytes
  - ShiftRows
  - AddRoundKey



Researchers have found a few potential ways to attack AES encryption. In 2009, they discovered a possible related-key attack. This cryptanalysis attempted to crack a cipher by studying how it operates using different keys. The related-key attack proved to be a threat only to AES systems that are incorrectly configured.

The year 2009 also saw a known-key distinguishing attack against AES-128. A known-key was used to discern the structure of the encryption. However, the hack only targeted an eight-round version of AES-128, rather than the standard 10-round version, making the threat relatively minor.

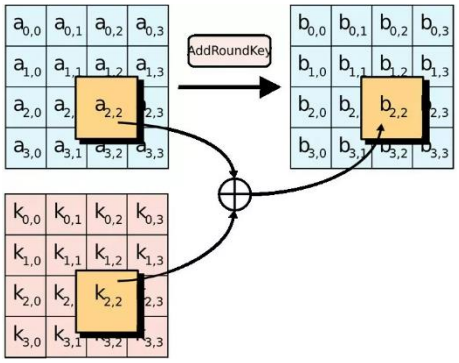
A major risk to AES encryption comes from side-channel attacks. Rather than attempting a brute-force assault, side-channel attacks are aimed at picking up leaked information from the system. Side-channel attacks, however, may reduce the number of possible combinations required to attack AES with brute force. Side-channel attacks involve collecting information about what a computing device does when it is performing cryptographic operations and using that information to reverse-engineer the device's cryptography system.

Mathematically, AES encryption security assumes that it will take an unfeasible amount of time by an adversary to crack the ciphertext without knowing the key. The underlying assumption of the given statement is that the adversary has knowledge of the ciphertext, the encryption algorithm, and the decryption algorithm. Side channel attack provides insight into the intermediate values which makes it easier to attack the AES algorithm for secret key.

2.2 Algorithms within AES

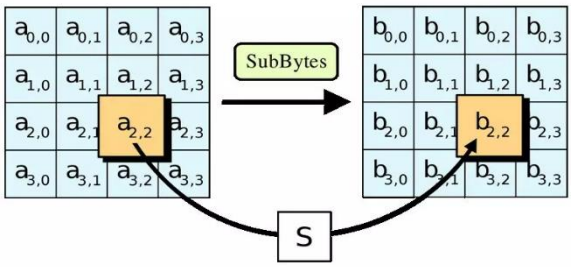
Secret Key in AES is either 128, 196, or 256 bits. In our lab we will be dealt with 128-bit key system which is more robust for device requiring low power consumption and/or low latency.

Ciphertext is generated in AES by a series of mathematical transformation involving plaintext and secret key as the starting point-



I. Key expansion:
Uses the original secret key to derive a series of new "round keys" using the Rijndael's key schedule algorithm

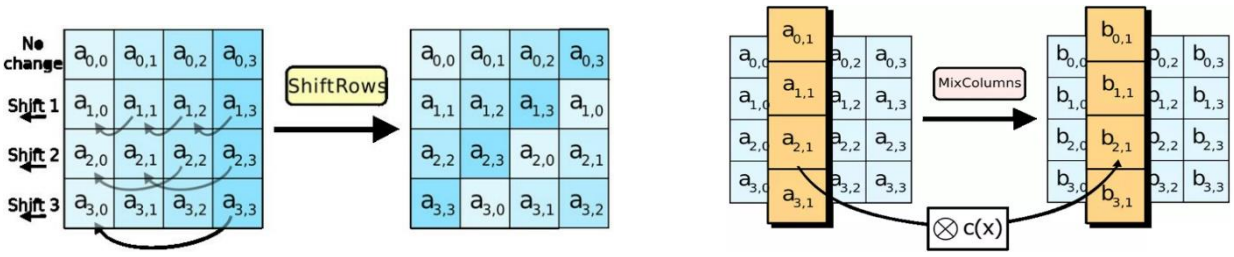
II. Add Round Key /Mixing:
The key expansion created in the earlier step is added to the plaintext using simple bitwise XOR algorithm. The output is then used to carry out 9 rounds (for AES-128) of further computations.



III. Sub Bytes Step/ Substitution Step:
Each byte $a_{i,j}$ in the state array is replaced with a *SubByte* $S(a_{i,j})$ using an 8-bit substitution box. This operation provides the non-linearity in the cipher. he S-box is also chosen to avoid any fixed points. 16 bytes of intermediate state gets transformed to 16 bytes of S-Box output. S-box operation is a simple look-up table with 256 values. Output of the S-box is the intermediate value we use for the attack vector.

IV. Shift Rows Step:
Operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset. Every byte in the 4 x 4 column of sixteen bytes that makes up a 128-bit block is shifted to the right.

V. Mix Columns Step:
Together with ShiftRows, MixColumns provides diffusion in the cipher.



2.3 Power Side channel attack and attack on AES-128

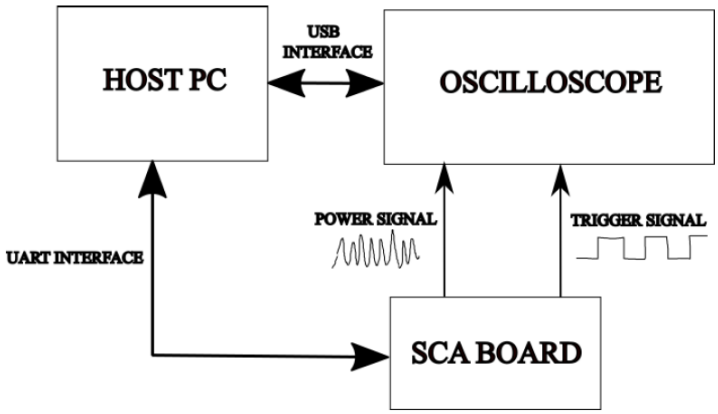
Power-side channel attacks(SCAs) are carried out by measuring and analysing power consumption of a chip/processor in the midst of encryption/decryption algorithm. The additional information gained by such attacks help in the cryptanalysis by providing additional information about the intermediate steps which in turn makes cryptanalysis and breaking the key easier. Generally, CMOS chips are targeted for such an attack vector. In

CMOS processor, there is additional power consumption for changing charge of capacitor compared to maintaining a steady state. In other words, a 0 -> 1 or 1->0 transition in the short-term memory will require more power consumption. The power consumption is then logically proportional to the bits transition i.e. more power consumption implies a greater number of bits change. That is:

Power consumption **α (**Total number of bits –Hamming weight**) α (**-Hamming Weight**)**
After collecting the data an Correlation Power Analysis is performed to determine the exact change of charge/power consumption and relate it to data captured.
Power-side channel attack is carried out in AES-128 to acquire knowledge about intermediate output of SubBytes Step. Power measurements/ power traces from an AVR 8-bit microcontroller mounted on a custom Side Channel Attack (SCA) evaluation board are collected and analysed to gauge an idea about the key.
SBOX(M` ⊕ K) = Y (intermediate output)

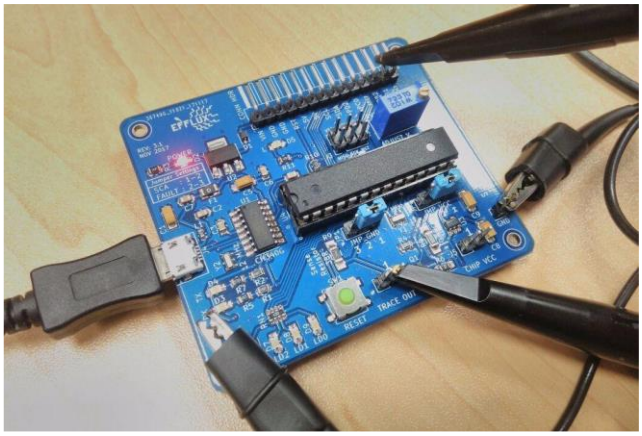
3. Lab proceedings

There are two major steps involved in performing power-SCA: gaining access to hardware and operating to obtain power traces.



Hardware required: Oscilloscope (Tektronix TDS2012C oscilloscope), Voltage probes, SCA board (Efflux SCA custom board)
Software required: SCA328P_Ctrl software tool, Power Analysis Tool (PAT)

As seen in the diagram, the PC is connected to the Oscilloscope via USB. SCA328P_Ctrl software tool is installed on the PC and is used to configure and control the scope remotely via PC. SCA board contains an 8-bit AVR ATMega328P microcontroller (MCU) which is flashed with firmware that runs AES algorithm on it. The board is connected to the PC through a UART interface using a USB cable.
The Efflux SCA Evaluation Board was designed and developed for the purpose of physical attack experiments (both side-channel and fault) within a single cryptographic circuit implemented on a micro-controller. To control the scope, remote commands from custom software tool SCA328P_ctrl is used to configure and operate the scope for displaying and collecting waveforms. The scope can measure the power consumption of the MCU on the SCA board through voltage probes connected to appropriate outputs on the SCA board. The SCA328P_Ctrl software triggers the MCU on the SCA board to run the secure algorithm. The SCA board further triggers the scope by raising a trigger signal during its operation which prompts the scope to capture the corresponding power consumption measurements as power traces.



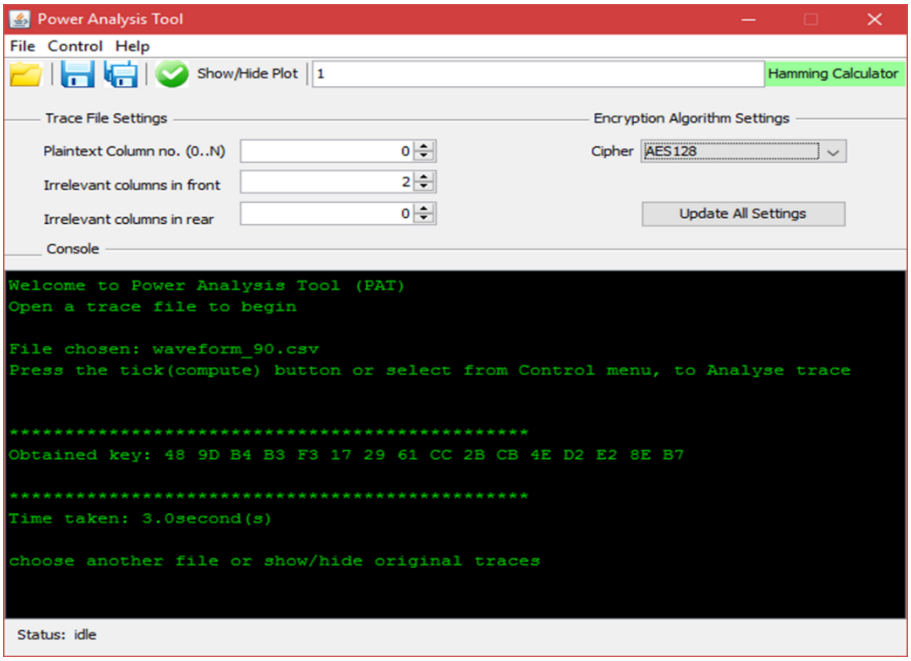
3.1 Steps used for power-trace collection

The pins and probes are connected on the SCA board as shown in figure above. The firmware in the MCU is configured to send a high signal when the waveform is to be measured which in our case is the first round of AES128 calculations.

Once the oscilloscope is connected to the PC, SCA328p_ctrl software is run. After receiving "Scope Connected, All Settings Applied!" message, we use the tool to establish connection with the SCA board since the tool has not established connection with the SCA board, all the control buttons on the pane are inactive. Key is updates according to user's need.

Test cases are run to conform that connection is established in all parts. AES128 encryption with random plaintexts are performed where oscilloscope should display the power and trigger waveforms on the scope display.

The traces collected are analysed using Power Analysis Tool (PAT) which runs the CPA algorithm on traces and extracts the key for AES128. The Correlation Power analysis attack on the AES-128 algorithm works based on a divide and conquer strategy to retrieve the used secret key for encryption. Then, the correlation between the traces and the hypothetical power consumption is calculated for all the key hypothesis and the hypothesis with the maximum correlation value is retrieved as that byte of the full key. The Leakage model



typically used in a micro-controller is the hamming weight leakage model. Leakages from the register writes during operation and the hamming weight of the written data are exploited. The type of attack performed is Chose Plaintext Attack.

The PAT is written in Java and is operated via a GUI. The trace file to be analysed has the first column as plaintext, second column as ciphertext and rest of the column as power traces. Sufficient number of traces are needed for accurate cracking of key. The key is retrieved 1 byte at a time. A model power consumption profile is built for every byte which is matched with collected data. A correlation matrix of dimension (256x2500) is used to analyse the correlation peak.

4. Conclusion

In lab 1 and 2 we foresaw power of side channel attack and various methods that can be used to break a "secure" encryption system. AES, despite being secure enough to be used for US government top secret documents, can be broken via power analysis tool built upon the method of correlation. The lab also provided insight on how to deter side-channel attack on a processor such as using randomized jittering/power consumption.