Lab 3: Fault Attacks -- Due date: 03/19/2020 11:55 PM

Overview:

The goal of this assignment is to act as a hardware hacker in the real world and deduce the secret keys of AES crypto-hardware using two different fault attacks.

Scenario:

Suppose that you found two suspicious devices in your office. By intercepting their network packets, you noticed that they send encrypted messages to a server abroad. You know that both of the devices are using AES-128 for encryption, and they are using different secret keys for encryption. You decide to crack the encryption on these two devices, so you ask for help from a friend (Bob, a physics guy) who can inject faults into the encryption process using laser shots. Unfortunately, he does not understand anything about security. Your friend has done a great job in injecting faults as you requested, so he gives to you a collection of correct and faulty ciphertexts. Now it's your job to figure out the secret key.

Reading Materials:

It is highly recommended that you start early to understand the research papers that outline the attacks:

[1] Giraud, Christophe. "DFA on AES." *International Conference on Advanced Encryption Standard*. Springer, Berlin, Heidelberg, 2004.
URL: https://link.springer.com/chapter/10.1007/11506447_4

[2] Mukhopadhyay, Debdeep. "An improved fault based attack of the advanced encryption standard." *International Conference on Cryptology in Africa*. Springer, Berlin, Heidelberg, 2009.
URL: https://link.springer.com/chapter/10.1007/978-3-642-02384-2_26

Lab Assignments:

You will be given two groups of ciphertexts. Each group contains correct/faulty ciphertexts that encrypt **the same 128-bit plaintext using the same 128-bit key**. Please note: the ciphertexts in this lab assignment are **unique** for each group.

1. When Bob was collecting all the faulty ciphertexts in the first group, he injects a **single bit flip fault** into **one** of the 16 bytes of M^9 (the input of the **10th round** of AES-128). In this way, he collected eighty faulty ciphertexts and one correct ciphertext, **all encrypting the same plaintext with the same key**.
2. In the fault injection experiments of the second group, Bob managed to inject **a byte fault** in **one** of the **4 bytes in the top row** of M^8 (the input of the **9th round** of AES-128). The concept of the top row will be explained in an example later. **We do not know how many bits are flipped in each one-byte fault.** After each fault injection, he let the encryption complete the remaining operations to collect the faulty ciphertexts, which are the outputs of the 10th round. By repeating this procedure, he collected twenty faulty ciphertexts and one correct ciphertext, **all encrypting the same plaintext with the same key**.

For this lab, your tasks are:

1. Understand the attack described in [1] Section 3 (hereafter referred to as “Bit Fault Attack”).
2. From the first group of correct/faulty ciphertexts, select the ciphertexts that can be used to recover one byte of the targeted round key, according to the fault patterns in the faulty ciphertexts.
3. Implement the bit fault attack on the selected ciphertexts to recover the targeted round key.
4. Understand the attack described in [2] Section 4 (hereafter referred to as “Byte Fault Attack”)
5. From the second group of correct/faulty ciphertexts, select the ciphertexts that are useful for you to attack four bytes of the targeted round key, according to the fault patterns in the faulty ciphertexts.
6. Implement the byte fault attack on the selected ciphertexts to recover the targeted round key.
7. Reverse engineer the round keys from the two fault attacks to 128-bit secret keys.
8. Write a report on how you select the ciphertexts for your attacks, and how you deduce the round key and further reverse-engineer the secret key.
9. Submit your results along with your attack implementation

Further instructions:

- Please pay attention to the order of the bytes in a state in AES encryption. An example is given below.
- **Easter Egg:** There is an Easter egg hidden in this lab. If you find it, you will get a chance to verify one of your recovered secret keys before submission. If nobody finds it, it will be announced after the lab due date. It is impossible to find the Easter Egg without completing the whole lab. Please first finish the lab.
- **Hint for the Easter Egg:** Why do you attack encryption methods? Please contact chenglu.jin@nyu.edu to verify your findings.
- **Happy hacking!**

An Example of An AES Block:

An intermediate state/ plaintext/ ciphertext of AES can be considered as a 4 by 4 block, which facilitates the visualization of ShiftRow and MixColumn operations.

For example, the state is 0x00112233445566778899AABBCCDDEEFF. Its block representation looks like below.

00	44	88	CC
11	55	99	DD
22	66	AA	EE
33	77	BB	FF

Note: All the faults injected for the byte fault attack are only injected in one of the bytes in the top row (0x00, 0x44, 0x88, or 0xCC in the above example).

Deliverables:

The following deliverables have to be submitted in a zip file format with lab3_<team_number>.zip

- Fault attack source code
- Lab report containing a description of your solution and analysis, including
  - Diagrams that show the propagation of faults after the fault injections
  - Diagrams that show how the propagation of faults will be affected by the location of the fault injections. E.g., How will the faults propagate differently if the faults are injected at the first byte of M^8 (0x00 in the above example) and the fifth byte of M^8 (0x44 in the above example), respectively?
  - Description of how the corresponding faulty ciphertexts are chosen from each group for attacking a part (a byte or a few bytes) of the targeted round key. Also, please specify which round's round key is the target in these two attacks.
  - Your recovered targeted round keys and the description of how you use the faulty ciphertexts to attack each byte (e.g., the equations used).
  - Your recovered secret keys and the description of how you reverse-engineer the secret keys from round keys.

A detailed assessment rubric will be provided at a later point