University of Maryland Baltimore County
CMPE/ENEE 691
Hardware Security
Spring 2023

HW5: Differential Fault Attack (DFA)
Due Date: 03/28/2023

Deliverables

- A .zip file containing
  1. Your script
  2. A ReadMe describing how to run your script
  3. A Makefile if applicable
  4. A file containing all round keys: round 0 → round 10

In this lab you will implement the Differential Fault Attack (DFA) presented in [1] on the Advanced Encryption Standard (AES) to find the encryption key.

The fault attack has launched on the input of round 10 in an AES crypto core. The fault model is bit-fault (only one bit in each byte can be faulty)

Assume you obtain the following fault free ciphertext and faulty ciphertexts.

1. Fault free ciphertext

```
f6  21  5a  c5
b1  ec  cb  1c
08  ba  cc  48
c1  13  37  d1
```

2. Three faulty ciphertexts:

   1st faulty ciphertext

```
5d  ba  6b  68
af  4d  04  1d
71  95  2b  7e
d4  5f  7d  13
```

   2nd faulty ciphertext

```
f0  c7  70  ce
29  38  e7  dc
73  1f  b0  d1
46  44  ec  87
```

   3rd faulty ciphertext

```
81  5f  8f  56
e9  d4  bf  8a
dd  40  39  bf
f2  d6  0d  97
```

Note that the faulty free and faulty ciphertexts were generated using the same input plaintext and key. **For each faulty ciphertext, 1-bit fault has-been injected in each byte of the round-10 input.**

You need to implement DFA (lecture 6 slide 30) attack to recover the round-10 key. Then, as the next step, derive the round-0 key from the round-10 key by implementing the inverse of the key schedule function (lecture 3 slide 63).

To verify your results, you can use an AES implementation and apply your round0-key with the following input plaintext. Then, as the output you should get the fault free ciphertext. You don't need to implement AES for this assignment. Alternatively, you can plug in your values in the online tool at https://www.cryptool.org/en/cto/aes-step-by-step in ECB mode or use any other tool or script of your choice.

Input plaintext

```
ff  ff  ff  ff
ff  ff  ff  ff
ff  ff  ff  ff
ff  ff  ff  ff
```

Note: You can use any programming/scripting language in this homework.

[1] C. Giraud, "DFA on AES," in IACR e-print archive 2003/008, p. 008, http://eprint.iacr.org/2003/008, 2003.