ECEN 759 Lab 7: Differential Fault Analysis Attack on AES

S M Farabi Mahmud

May 6, 2021

1 Single Bit Fault Attack

In this section, we will describe how we have implemented the single bit fault attack on AES. We used the concept from Giraud's work [**?**]

2 Byte Fault Attack