CS741 Assignment 2 - Q1 Report

Neel Aryan Gupta 180050067

Pulkit Agrawal 180050081

Tathagat Verma 180050111

Time complexity = $O(2^8 * 2^8 * 2^8 * 8\ ) \ = \ O(2^{27})$

Explanation: First 2^8 is iterating over all possible sets of input bits (whose bias we want).
Second 2^8 is iterating over all possible sets of output bits (whose bias we want).
Third 2^8 is iterating over all possible values of the input-output pairs of sbox.
Last 8 (number of input bits to the S-Box) is for taking the XOR of all required bits.

Time for program to run:
~ 10 sec (to calculate and save biases in a txt file when run for the first time)
~ 2 sec (all the subsequent runs where the precalculated bias is loaded from the txt file)

The biases are even because:
Consider AES S-Box drawn in tabular form which has 256 rows and 16 columns(8 for input bits and 8 for output bits). As S-box is a bijective function, all 256 values (ranging from 0 to 255) appear once in the input and output. Therefore, take any 1 column of the 16 columns: It would have “1” 128 times and “0” 128 times.

Consider any set “a” of input bits and any set “b” of output bits (|a| >= 1 and |b| >= 1). For example a = {I1, I2, I3} and b = {O1, O2}. Thus, the total number of “1” appearing in the sets “a” and “b” combined is 128(|a|+|b|) [which is an even quantity].

Now, let's suppose that the bias count is odd. It implies that the number of rows (out of 256) whose xor is zero is odd. Therefore, the number of rows (out of 256) which has an even number of “1” is odd. (because xor = 0 => number of ones is even).

As there are a total of 256 rows, the remaining number of rows (containing an odd number of “1”) is also odd. (because odd + even ≠ 256).

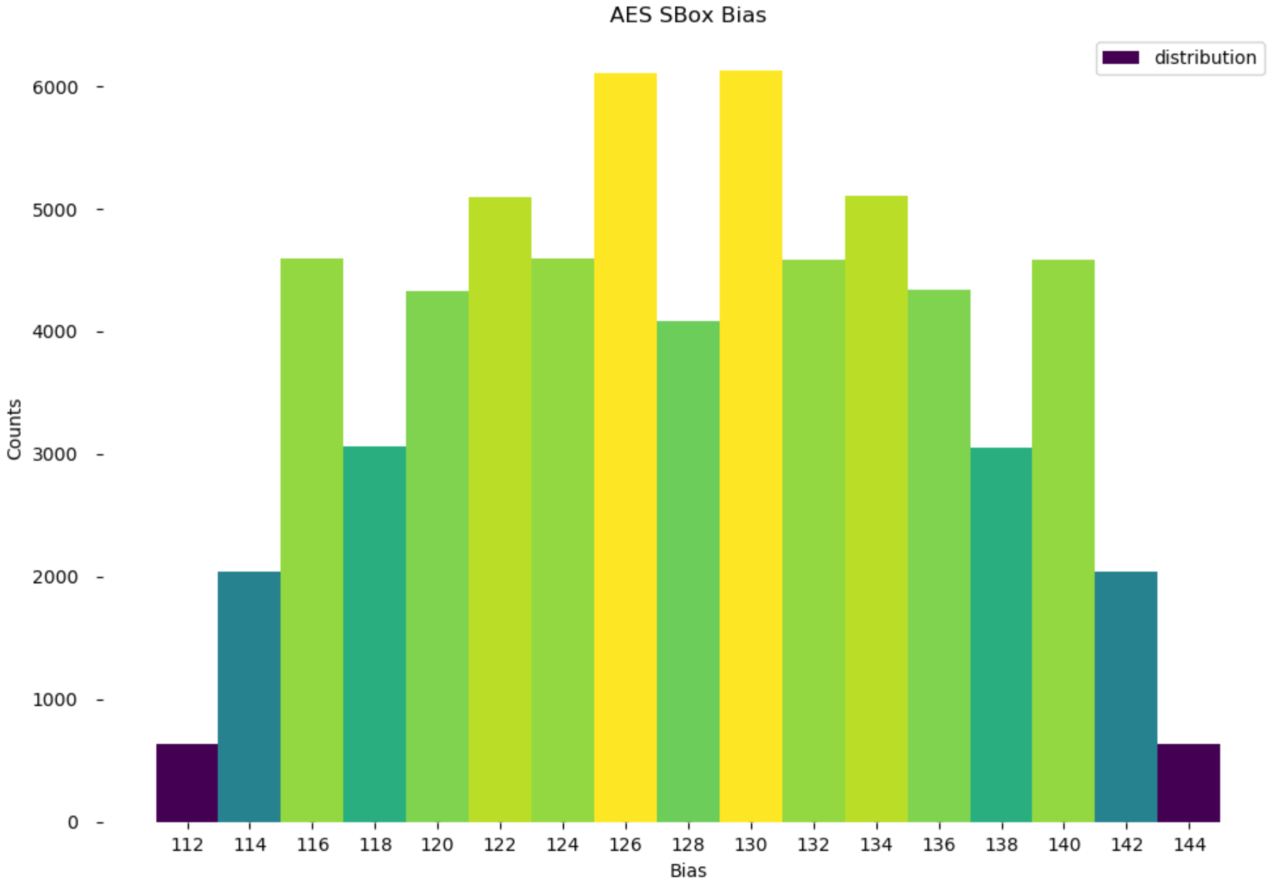
Thus, Total number of “1” in the selected sets “a” and “b” = (odd*even) + (odd*odd).
We know odd*even = even, odd*odd = odd and even+odd = odd. We conclude that the total number of “1” is odd. But we showed earlier that total number of “1” in sets “a” and “b” is 128(|a|+|b|) which is even. Hence a Contradiction!

Therefore, the number of rows where xor is zero is even. That implies that the bias is always even.

Bias Table

Bias	Combinations
112	640
114	2040
116	4592
118	3064
120	4334
122	5096
124	4592
126	6112
128	4080
130	6128
132	4588
134	5104
136	4336
138	3056
140	4588
142	2040
144	635

Histogram


AES SBox Bias
distribution
Counts
6000
5000
4000
3000
2000
1000
0
112
114
116
118
120
122
124
126
128
130
132
134
136
138
140
142
144
Bias