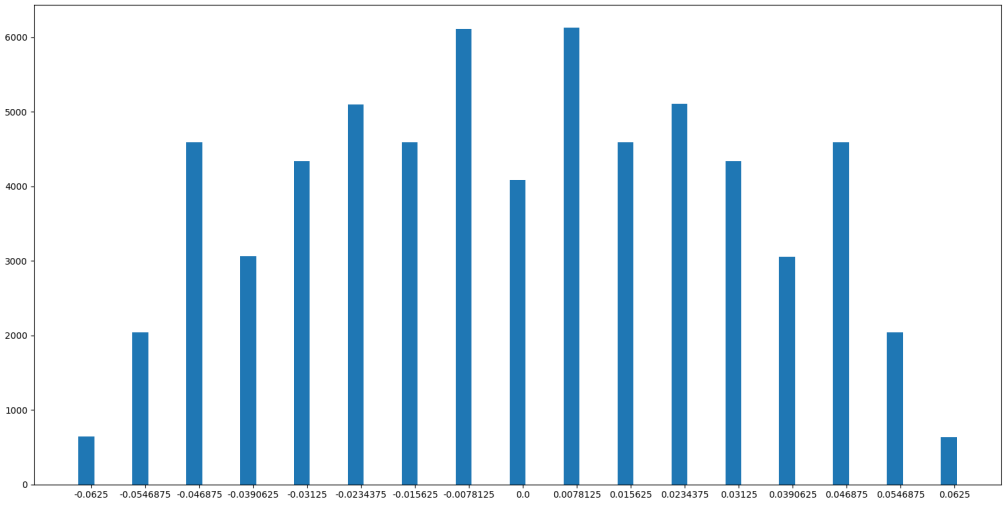
Histogram:



The above figure displays bias on the X-axis and the number of combinations on the Y-axis

Bias Table:

Bias	Number of combinations
-0.0625	640
-0.0546875	2040
-0.046875	4592
-0.0390625	3064
-0.03125	4334
-0.0234375	5096
-0.015625	4592
-0.0078125	6112
0.0	4080
0.0078125	6128
0.015625	4588
0.0234375	5104
0.03125	4336
0.0390625	3056
0.046875	4588
0.0546875	2040
0.0625	635

The reason for bias to be even positive integer:

Page No.
Date / /

Suppose if mask have even elements then expression would be similar to

$a \oplus b \oplus c \oplus d$

Suppose a configuration like (0,1,0,1) gives

$0 \oplus 1 \oplus 0 \oplus 1 = 0$ then ∃ another configuration by bit flipping which also gives 0

Bit flipping of (0,1,0,1) gives (1,0,1,0)

$1 \oplus 0 \oplus 1 \oplus 0 = 0$

Suppose if mask have odd elements then expresion would be similar to

$a \oplus b \oplus c \oplus d \oplus e$ → ①

Suppose a configuration like (0,1,0,1,0) gives

$0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 = 0$, then ∃ (# of zeros of ①) other configurations which also gives 0

$0 \oplus 0 \oplus 1 \oplus 0 \oplus 1 = 0$
$1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 = 0$
$1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 = 0$

} formed by fixing 1 0 and bit flipping other bits

# of zeros of ① would be odd since xor of all bits of ① is 0 ⇒ odd +1 ⇒ even number of configurations on xor of all of its bits gives 0.

Hence the biases are positive even integers

Time Complexity:

Time Complexity of the code is $O(2^8 * 2^8 * 2^8 * 16) = O(2^{28})$

- $(2^8 - 1)$ combinations of inputs are possible
- $(2^8 - 1)$ combinations of outputs are possible
- 2^8 elements in the S-box
- $O(16)$ computations for finding the XOR of all bits of a 16-bit number

Approximate average time taken to complete the execution of the program (including generating histogram) is **10** seconds