CSE 667 Assignment 2: S-Box Explanation

Caleb Alexander, Matthew O'Connor, Ryan Holthouse, Huy Tran, Mathan Patel

1 Bent Functions

Our S-box will be constructed using "bent" functions. A bent function is one which satisfies the following properties:

- The function is boolean. ($|Codomain(f)| = 2$)
- The function disagrees with all linear functions on its domain **maximally**.

A more formal way of writing the second condition is that for a bent function $F : D \to C$, the following quantity

$$H(f(x), l(x)) \quad \text{where } x \in D \text{ and l is some linear function from } D \text{ to } C.$$

is maximized across all x and all l (Note: H is the usual hamming distance, so it is the count of bits that disagree).

By their non-linear nature, bent functions make good candidates in the construction of an S-Box. It has been proven that

$$f((x_1, x_2)) = x_1x_2 \quad \text{concatenation is multiplication mod 2}$$

is bent in $GF(2)$. Furthermore the addition of bent functions is bent, so a function such as

$$f((x_1, x_2, x_3, x_4)) = x_1x_2 \oplus x_3x_4$$

is also bent. In general, for an n-length bitstring

$$\textbf{if} \quad x = (x_1, x_2, x_3, \ldots, x_n) \quad \textbf{then} \quad f(x) = x_ax_b \oplus x_cx_d \oplus \cdots \oplus x_ix_j$$
$$\textbf{where} \quad a, b, c, d, \ldots, i, j \in \{1, \ldots, n\} \wedge a \neq b \neq c \neq \cdots \neq j$$

are bent functions.

We have constructed and will be using the following bent functions,

$$\begin{aligned}
f_1(x) &= x_1x_2 \oplus x_3x_4 \oplus x_5x_6 \oplus x_7x_8\\
f_2(x) &= x_1x_3 \oplus x_2x_4 \oplus x_5x_7 \oplus x_6x_8\\
f_3(x) &= x_1x_4 \oplus x_2x_3 \oplus x_9x_{10} \oplus x_{11}x_{12}\\
f_4(x) &= x_5x_6 \oplus x_7x_8 \oplus x_{13}x_{14} \oplus x_{15}x_{16}\\
f_5(x) &= x_9x_{10} \oplus x_{11}x_{12} \oplus x_1x_5 \oplus x_2x_6\\
f_6(x) &= x_3x_7 \oplus x_4x_8 \oplus x_{13}x_{15} \oplus x_{14}x_{16}\\
f_7(x) &= x_1x_9 \oplus x_2x_{10} \oplus x_3x_{11} \oplus x_4x_{12}\\
f_8(x) &= x_5x_{13} \oplus x_6x_{14} \oplus x_7x_{15} \oplus x_8x_{16}\\
f_9(x) &= x_1x_6 \oplus x_2x_5 \oplus x_3x_8 \oplus x_4x_7\\
f_{10}(x) &= x_9x_{14} \oplus x_{10}x_{13} \oplus x_{11}x_{16} \oplus x_{12}x_{15}\\
f_{11}(x) &= x_1x_{14} \oplus x_2x_{13} \oplus x_3x_{16} \oplus x_4x_{15}\\
f_{12}(x) &= x_5x_{10} \oplus x_6x_9 \oplus x_7x_{12} \oplus x_8x_{11}\\
f_{13}(x) &= x_9x_6 \oplus x_{10}x_5 \oplus x_{11}x_8 \oplus x_{12}x_7\\
f_{14}(x) &= x_1x_{11} \oplus x_2x_{12} \oplus x_3x_9 \oplus x_4x_{10}\\
f_{15}(x) &= x_5x_{15} \oplus x_6x_{16} \oplus x_7x_{13} \oplus x_8x_{14}\\
f_{16}(x) &= x_{13}x_2 \oplus x_{14}x_1 \oplus x_{15}x_4 \oplus x_{16}x_3
\end{aligned}$$

we will consider

$$S(x) = \big(f_1(x), f_2(x), f_3(x), \ldots, f_{16}(x)\big).$$

2 Achieving Balance

Notice that using the current S could result in outputs that are not necessarily secure in a few ways. The first thing that we ought to protect against is the chance that $S(x) \in \{000\ldots00, 111\ldots111\}$. To protect against this, we construct a random non-repeating vector b, of length 16×1.

Next we want our output to be relatively balanced, meaning that an output should have a similar number of 0's and 1's. To assure this we must construct a 16×16 sized matrix, A, which should be invertible and have good cryptographic properties. An explanation of those properties and how to achieve them is outside the scope of this report. However, we took our matrix from Algebraic Construction of 16×16 Binary Matrices of Branch Number 7 with One Fixed Point, and it provides a great explanation. Our final output for a given input x will be

$$S'(x) = A \cdot S(x) + b \mod 2$$

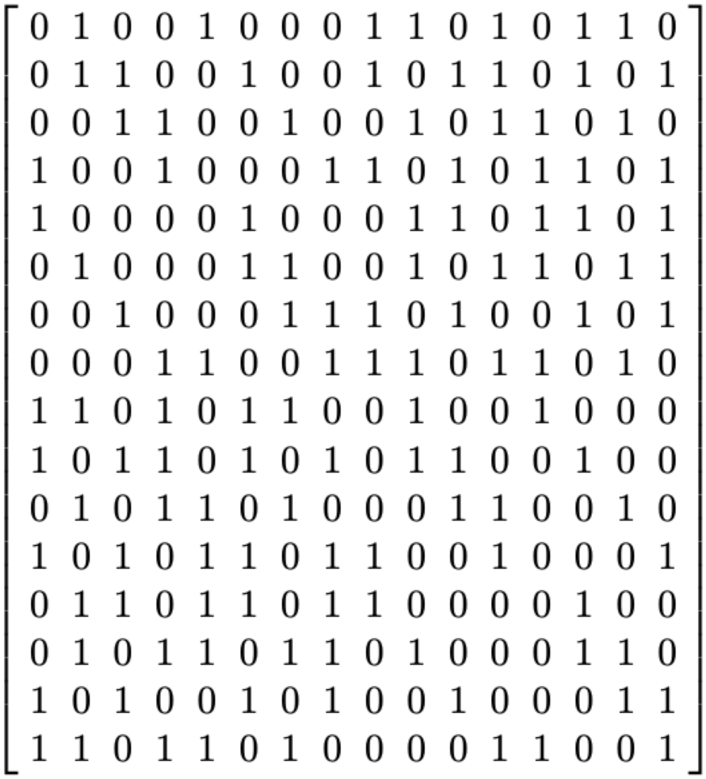
where $A \cdot S(x)$ is the usual matrix-vector multiplication.

Below our choice for b and A are included.

2.1 A and B

$$b = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

A is below.



$$\begin{bmatrix}
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1
\end{bmatrix}$$

This is taken directly from Algebraic Construction of 16×16 Binary Matrices of Branch Number 7 with One Fixed Point.