CS553 Cryptography

BitBees

Question 3

Boolean Functions for S-Box

For the implementation part, please refer to `DDT.ipynb`

S-Boxes are boolean mappings from

$$\{0,1\}^m \to \{0,1\}^n$$

A total of $m \times n$ mappings. Thus there are a total of n component functions each being a map from m bits to 1 bit.

A boolean function in n inputs (4 in our case) can be represented as a sum of XORs and ANDs.

Algebraic Normal Form (ANF) is the canonical form of the boolean function.

In Sage, `component_function(b)` returns the component function corresponding to $b.S(x)$. There are a total of 16 component functions for a 4-bit S-Box. For our S-Box here are all the component functions in ANF.

`x0*x1*x2 + x0*x1*x3 + x0*x2*x3 + x0*x2 + x0*x3 + x1*x2*x3 + x2*x3 + x2 + x3 + 1`

`x0*x1*x2 + x0*x2*x3 + x0*x2 + x0 + x1*x3 + x1 + x2 + x3 + 1`

`x0*x2*x3 + x0*x3 + x1 + x2 + x3 + 1`

`x0*x1*x2 + x0*x1*x3 + x0*x3 + x0 + x1*x2 + x1*x3 + x2*x3 + x3`

Here each function represents a bit of our S-Box output.