Example

Consider the parity function

$$p_3 : \mathbb{F}_2^3 \to \mathbb{F}_2 \quad \text{on 3 variables}$$

outputs 0 if even
1 if odd

	x_1	x_2	x_3	$p_3(x_1, x_2, x_3)$	
$p_3(000)$	0	0	0	0	f_0
$p_3(001)$	0	0	1	1	f_1
$p_3(010)$	0	1	0	1	f_2
$p_3(011)$	0	1	1	0	f_3
$p_3(100)$	1	0	0	1	f_4
$p_3(101)$	1	0	1	0	f_5
$p_3(110)$	1	1	0	0	f_6
$p_3(111)$	1	1	1	1	f_7

TT Truth Table

$n = 40 \rightarrow 2^{40} = 128\,Gb$ to much space

⇓

ANF Algebraic Normal form

$f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$

a polynomial over $\mathbb{F}_2$ with n indeterminates

$$f(x_1 x_2 \dots x_n) = a_0 + a_1 x_1 + a_2 x_2 + a_3 x_1 x_2 + \dots + a_{2^n-1} x_1 x_2 \dots x_n$$

$a_i \in \mathbb{F}_2 \quad \{0,1\}$

ANF can have 2^n terms

$p_3(x_1, x_2, x_3) = x_1 + x_2 + x_3$

$p_3(0\ 1\ 1) = 0 + 1 + 1 = 0$ ($\mathbb{F}_2$)

Conversion ANF → TT representation is evaluating the polynomial

An important statistic (a numerical piece of information) of the Boolean function that can be immediately extracted from ANF is its so called algebraic degree.

high algebraic degree →
good resistance to high order differential attacks

The algebraic degree of a Boolean function is the degree of its ANF

is the number of indeterminates in the largest term with a non zero coefficient.

Eg. $f(x_1 x_2 x_3 x_4) = 1 + x_2 + x_1x_3 + x_1x_2x_4$

(2 vars; 1 var; 3 vars)

indeterminates → variables

since the largest group is $x_1x_2x_4$ the algebraic degree of $f = 3$.

Functions of algebraic degree 1, resp 2, resp 3 are referred to as

1 = affine → affine with no constant term is called linear.
2 = quadratic
3 = cubic

TT to ANF

one way through atomic functions

Atomic functions is a Boolean function that evaluates to 1 for precisely 1 input.

$$f(x) = \begin{cases} 1, & 1 \\ 0, & 2^n - 1 \end{cases}$$

TT in Example 1

evaluates to 1 for

$p_3(x_1 x_2 x_3) = (0\,0\,1) : f_1$

$= (0\,1\,0) : f_2$

$= (1\,0\,0) : f_4$

$= (1\,1\,1) : f_7$

$$f_1(x_1x_2x_3) = \begin{cases} 1, & (x_1x_2x_3) = (0,0,1) \\ 0, & - \end{cases}$$

$$f_2(x_1x_2x_3) = \begin{cases} 1, & (x_1x_2x_3) = (0\,1\,0) \\ 0, & - \end{cases}$$

$$f_4(x_1x_2x_3) = \begin{cases} 1, & (x_1x_2x_3) = (1\,0\,0) \\ 0, & - \end{cases}$$

$$f_7(x_1x_2x_3) = \begin{cases} 1, & (x_1x_2x_3) = (1\,1\,1) \\ 0, & - \end{cases}$$

$$P_3 = f_1 + f_2 + f_4 + f_7$$

Systematic approach

F_2

$$(x_1+1)(x_2+1)x_3$$

If $x_1 = 1 \Rightarrow (x_1+1) = (1+1) = 0$

the entire poly evaluates to 0.

$$\left.\begin{array}{l} x_1 = 0 \\ x_2 = 0 \\ x_3 = 1 \end{array}\right\} (x_1x_2x_3) = (0,0,1)$$

$$f(x_1, x_2, x_3) = (x_1 + 1)(x_2 + 1)x_3$$

$$(x_1 x_2 + x_1 + x_2 + 1)\, x_3$$

$$f_1(x_1, x_2, x_3) = x_3 + x_3 x_2 + x_3 x_1 + x_3 x_1 x_2$$

$$f_2(x_1, x_2, x_3) = (x_1 + 1)\, x_2\, (x_3 + 1)$$

$$= x_2 + x_1 x_2 + x_2 x_3 + x_1 x_2 x_3$$

And the ANF of p_3 =

$$p_3 = f_1 + f_2 + f_4 + f_8 = \quad =$$

$$= x_1 + x_2 + x_3$$ since FF_2

Vectorial Boolean functions

In general a boolean function outputs only one bit.

(n, m) functions

$F: \mathbb{F}_2^n \to \mathbb{F}_2^m$

eg

$F: \mathbb{F}_2^4 \to \mathbb{F}_2^2$ $\quad n=4, m=2$

regular boolean function is

(n, 1)

Example (3,2) TT

x_1	x_2	x_3	$F(x_1, x_2, x_3)$	
0	0	0	0	0
0	0	1	0	1
0	1	0	1	1
0	1	1	1	0
1	0	0	1	1
1	0	1	1	0
1	1	0	0	0
1	1	1	0	1

$F = (f_1, f_2)$

f_1 and f_2 are coordinate functions of F

Distance (Hamming distance)

How different two functions are from each other.

$$d(F,G) = |\{(x_1 x_2 \ldots x_n) \in \mathbb{F}_2^n \mid F(x_1 \ldots x_n) \neq G(x_1 \ldots x_n)\}|$$

Table 4, Hamming distance

$$d(F,G) = 4$$

inputs		
0,0,1	0,1	
0,1,1	1,0	④ ou
1,0,1	1,0	
1,1,1	0,1	

Univariate Poly. form

elements in $\mathbb{F}_{2^n}$ can be seen as n-dimentional vectors of $\mathbb{F}_2$ elements

Finite Field $\mathbb{F}_{2^n}$ and Vectorspace $\mathbb{F}_2^n$ are representing the same thing

When m divides n it allows us to represent (n,m)-functions as univariate polynomials over $\mathbb{F}_{2^n}$

since $x^{2^n} = x$, $\forall x \in \mathbb{F}_{2^n}$

degree is $2^n - 1$

$\Downarrow$

(n,m) function F in the form

$$F(x) = \sum_{i=0}^{2^n-1} a_i x^i \qquad a_i \in \mathbb{F}_{2^n}$$