3. Most biased linear functions.

probability distribution

$$P = (P_0, P_1, \dots, P_{2^n-1}), \quad P_i \geq 0 \quad \sum_{i=0}^{2^n-1} P_i = 1.$$

i	$X_1 X_2 \dots X_n$	P_i
0	0 0 ... 0	P_0
1	0 0 ... 1	P_1
	...	
2^n-1	1 1 ... 1	P_{2^n-1}

common notation $a = (a_1, \dots, a_n)$
$x = (x_1, \dots, x_n)$

linear Boolean function

$$a \cdot x = \sum_{i=1}^{n} a_i x_i$$

assume x taken from $\{0, 1, \dots, 2^n-1\}$ according to the distribution P.

$\Rightarrow$ $a \cdot x$ random variable

$$(*) \quad P_x(a \cdot x = 0) = \sum_{x:\, a \cdot x = 0} P_x = \frac{1}{2} + \delta_a$$

δ_a called bias.

task: **find $a \neq 0$ s.t. $|\delta_a|$ - max.**

trivial example. $a = 0$

$$1 = Pr(0 \cdot x = 0) = \sum_{x : 0 \cdot x = 0} P_x = \frac{1}{2} + \delta_0$$

$$\Rightarrow \delta_0 = \frac{1}{2}.$$

trivial solution

brute force a and x
compute $Pr(ax=0)$ by $(*)$.

takes $\approx 2^{2n}$ trials.

Apply Walsh-Hadamard transform and do that in $n \cdot 2^n$ operations.

WH tranform to probability vector P.

$$Y = P \cdot H_n =$$

H_n: Hadamard matrix of size $2^n \times 2^n$.

$$= \underline{(P_0 P_1 \ldots P_{2^n-1})} \times \begin{pmatrix} & a & \\ & \vdots & \\ \cdots & (-1)^{a \cdot x} & \cdots \end{pmatrix}$$

$$\Rightarrow Y_a = \sum_{x=0}^{2^n-1} P_x (-1)^{a \cdot x} =$$

$$= \sum_{x: ax=0} P_x - \sum_{x: ax=1} P_x = 2\delta_a$$

$$\left.\begin{aligned} \sum_{x: ax=0} P_x &= \frac{1}{2} + \delta_a \\ \sum_{x: ax=1} P_x &= \frac{1}{2} - \delta_a \end{aligned}\right\}$$

In order to compute $2 \cdot \delta_a$ for all $a = 0, \boxed{\dots, 2^n - 1}$ apply WH to P.

complexity $n \cdot 2^n$ add/subtr. with reals.

Example. $n = 3$

i	$x_1 x_2 x_3$	P_i
0	0 0 0	1/2
1	0 0 1	0
2	0 1 0	0
3	0 1 1	0
4	1 0 0	1/6
5	1 0 1	1/6
6	1 1 0	0
7	1 1 1	1/6

find lin. function $a \cdot x$ with largest $|\delta_a|$, $a \neq 0$

apply WH to the probabilities

$a =$	0 (000)	1 (001)	2 (010)	3 (011)	4 (100)	5 (101)	6	7
	$\frac{1}{2}$	0	0	0	1/6	1/6	0	1/6
	$\frac{1}{2}$	$\frac{1}{2}$	0	0	1/3	0	1/6	-1/6
	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$-\frac{1}{6}$	1/6	1/6
$2 \cdot \delta_a =$	(1)	1/3	2/3	2/3	0	2/3	1/3	1/3

trivial case $a=0$

$1 = P_2(a\cdot X=0) = \frac{1}{2}+\frac{1}{2} = 1$

$P_2(x_3=0) = \frac{1}{2}+\frac{1}{3\cdot 2} = \frac{4}{6} = 2/3$

best δ_a, $a=2,3,5$

$P_2(x_2=0) = \frac{1}{2}+\frac{1}{3} = \frac{5}{6} =$

$= P_2(x_1+x_2=0) = P_2(x_1+x_3=0)$

---

4. Vectorial Boolean Functions and S-Boxes

$S : n\text{-bit} \longrightarrow m\text{-bit}$

$S(X) = Y$

in DES $n=6,\ m=4$

AES $n=m=8$.

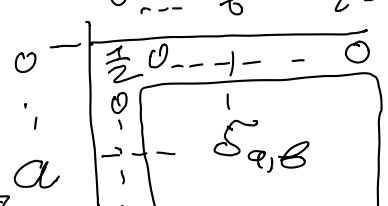
Assume x (input to S) is uniformly distributed on $0, 1, \dots, 2^n-1$

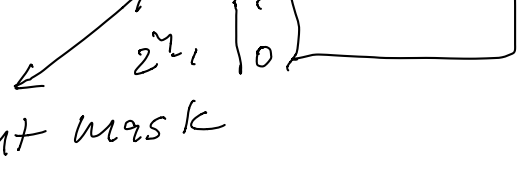
look at $a\cdot X + b\cdot Y = a\cdot X + b\cdot S(X)$

n-bit string ↑ m-bit string

$P_2(aX+b\cdot S(X)=0) = \frac{1}{2}+\delta_{a,b}$ → output mask.

table of $\delta_{a,b}$





task Find a, b s.t. $|\delta_{a,b}| \to \max$.

trivial cases

1) $a = 0, b = 0$

$$Pr(0 \cdot x + 0 \cdot S(x) = 0) = \frac{1}{2} + \frac{1}{2}$$

$$\Rightarrow \delta_{0,0} = \frac{1}{2}$$

2) $a \neq 0, b = 0$

$$Pr(\underline{a}x + 0 \cdot S(x) = 0) = \frac{1}{2} + 0$$

$$\Rightarrow \delta_{a,0} = 0, \quad a \neq 0.$$

3) if S-box is good enough (output uniformly destributed)

$a = 0, b \neq 0$

$$Pr(0 \cdot x + \underbrace{b \cdot S(x)}_{\text{balanced}} = 0) = \frac{1}{2} + 0$$

$$\Rightarrow \delta_{0,b} = 0$$

solve this computational problem with brute force

run over a, b, x (a: n-bit, b: m-bit, x: n-bit)

2^{m+2n} trials.

Apply WH transform and do

in $(m+n)\cdot 2^{m+n}$ add/subtr. with reals.

How to do?

construct probability distribution

on $(n+m)$-bit vectors

$$P_{x,y} = \begin{cases} 1/2^n & \text{if } y = S(x) \\ 0 & \text{otherwise.} \end{cases}$$

$$P = (P_{0,0}, \dots, P_{2^n-1, 2^m-1})$$

$$Y = P \cdot H_{n+m}$$

↑ Hadamard matrix of size $2^{n+m} \times 2^{n+m}$.

$$\Rightarrow Y_{a,b} = 2 \cdot \delta_{a,b}$$

Example. $n = m = 2$

x_1	x_2	y_1	y_2
0	0	1	0
0	1	0	1
1	0	1	1
1	1	0	0

probability vector

X_1	X_2	Y_1	Y_2	P
0	0	0	0	0
0	0	0	1	0
0	0	1	0	1/4
0	0	1	1	0
0	1	0	0	0
0	1	0	1	1/4
0	1	1	0	0
0	1	1	1	0
1	0	0	0	0
1	0	0	1	0
1	0	1	0	0
1	0	1	1	1/4
1	1	0	0	1/4
1	1	0	1	0
1	1	1	0	0
1	1	1	1	0

Pairs of $\delta_{\alpha,\beta}$ of length $2^{2+2} = 16$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	0	0	1	0	0	0	0	0	1	1	0	0	0
0	0	1	0	1	-1	0	0	0	0	1	-1	1	1	0	0
1	0	-1	0	1	-1	1	-1	1	-1	-1	1	1	1	1	1
2	-1	0	-1	0	1	-2	1	2	0	0	2	0	-2	-2	0
4	-1	0	1	0	-1	-4	1	0	-1	0	-3	0	3	0	1
1	-1/4	0	1/4	0	-1/4	-1	1/4	0	-1/4	0	-3/4	0	3/4	0	1/4

δ_{0110} - 1/4

$$2\delta_{01,10} = -1 \Rightarrow \delta_{01,10} = -\frac{1}{2}$$

$$P_2((01)\cdot(X_1X_2) + (10)(Y_1Y_2) = 0) =$$

$$= P_2(X_2 + Y_1 = 0) = \frac{1}{2} - \frac{1}{2} = 0$$

---

5. Compute convolutions

$$f, v : \{0, 1, \dots, 2^n - 1\} \longrightarrow \mathbb{R}$$

convolution of f, v

part of cipher key of length n.

$$C(k) = \sum_{x=0}^{2^n - 1} v(x) \cdot f(x \oplus k)$$

value of a statistic

$$\Rightarrow C : \{0, 1, \dots, 2^n - 1\} \longrightarrow \mathbb{R}.$$

compute all values of C.

in Linear Cryptanalysis of Block ciphers.

compute fast by WH transform.

$\overline{v}, \overline{p}, \overline{c}$ WH transforms of v, p, c

One proves

$$\overline{c}(k) = \overline{v}(k) \cdot \overline{p}(k)$$

$k = 0, \ldots, 2^n - 1.$

$$\Rightarrow \quad c = \frac{1}{2^n}\overline{(\overline{c})} = \overline{(\overline{v} \cdot \overline{p})}\,\frac{1}{2^n}$$

as $H_n \cdot H_n = \begin{pmatrix} 2^n & & 0 \\ & \ddots & \\ 0 & & 2^n \end{pmatrix}$.

compute convolution by 3 WH transform applications.