Criptoanálise Linear

Daniel Veiga da Silva Antunes

Junho 2023

1 Tabela de Bias

A partir da análise da S-BOX disponibilizada geramos a Tabela de Bias abaixo.

Tabela de Bias para SBOX (fator de 1/256)*

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**a**	**b**	**c**	**d**	**e**	**...**
1	-2	-6	-8	-14	-4	0	-6	-8	-10	-2	-4	2	4	-4	. . .
2	-12	-4	-8	-10	-10	-2	-10	0	16	-16	0	2	14	-2	. . .
3	-18	-10	4	4	18	2	0	4	-10	2	12	12	6	2	. . .
4	-12	16	-4	-6	-10	10	-10	2	-10	-10	2	-4	0	0	. . .
5	6	2	-8	-4	-2	2	-4	-6	0	4	-6	-2	0	12	. . .
6	0	0	0	-4	8	8	-4	-2	18	-2	10	-2	6	-6	. . .
7	-2	2	0	-14	8	-4	-6	2	-4	0	-14	0	-14	-10	. . .
8	2	-4	10	-14	0	-6	4	8	10	20	2	-2	4	6	. . .
9	12	2	2	4	8	-2	-10	0	-12	-10	-2	8	4	-10	. . .
a	-14	4	2	0	2	4	2	0	-10	8	2	0	-2	8	. . .
b	16	10	6	-2	2	-4	-4	-4	0	-10	-2	10	18	-8	. . .
c	14	-4	6	-12	-2	-20	-6	10	0	2	4	2	4	6	. . .
d	4	2	2	-2	2	-8	16	-6	-2	4	-12	12	-8	-2	. . .
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	

* Tabela completa disponível no anexo biastable.csv

2 Equações

Em seguida localizamos os maiores bias em módulo e selecionamos as fórmulas relativas a valores de X com peso de hamming = 1, afim de isolarmos um único K. Com isto obtemos 8 equações:

Para X = 128 (hamming: 1) e Y = 205 com um bias de 22 temos:

$$Pr[X_1 \oplus Y_1 \oplus Y_2 \oplus Y_5 \oplus Y_6 \oplus Y_8 = 0] = 0.586$$

$$K_1 = W_1 \oplus Y_1 \oplus Y_2 \oplus Y_5 \oplus Y_6 \oplus Y_8$$

Para X = 64 (hamming: 1) e Y = 110 com um bias de -28 temos:

$$Pr[X_2 \oplus Y_2 \oplus Y_3 \oplus Y_5 \oplus Y_6 \oplus Y_7 = 1] = 0.609$$

$$K_2 = W_2 \oplus Y_2 \oplus Y_3 \oplus Y_5 \oplus Y_6 \oplus Y_7 \oplus 1$$

Para X = 32 (hamming: 1) e Y = 77 com um bias de 24 temos:

$$Pr[X_3 \oplus Y_2 \oplus Y_5 \oplus Y_6 \oplus Y_8 = 0] = 0.594$$

$$K_3 = W_3 \oplus Y_2 \oplus Y_5 \oplus Y_6 \oplus Y_8$$

Para X = 16 (hamming: 1) e Y = 69 com um bias de 26 temos:

$$Pr[X_4 \oplus Y_2 \oplus Y_6 \oplus Y_8 = 0] = 0.602$$

$$K_4 = W_4 \oplus Y_2 \oplus Y_6 \oplus Y_8$$

Para X = 8 (hamming: 1) e Y = 99 com um bias de -20 temos:

$$Pr[X_5 \oplus Y_2 \oplus Y_3 \oplus Y_7 \oplus Y_8 = 1] = 0.578$$

$$K_5 = W_5 \oplus Y_2 \oplus Y_3 \oplus Y_7 \oplus Y_8 \oplus 1$$

Para X = 4 (hamming: 1) e Y = 94 com um bias de 22 temos:

$$Pr[X_6 \oplus Y_2 \oplus Y_4 \oplus Y_5 \oplus Y_6 \oplus Y_7 = 0] = 0.586$$

$$K_6 = W_6 \oplus Y_2 \oplus Y_4 \oplus Y_5 \oplus Y_6 \oplus Y_7$$

Para X = 2 (hamming: 1) e Y = 255 com um bias de 26 temos:

$$Pr[X_7 \oplus Y_1 \oplus Y_2 \oplus Y_3 \oplus Y_4 \oplus Y_5 \oplus Y_6 \oplus Y_7 \oplus Y_8 = 0] = 0.602$$

$$K_7 = W_7 \oplus Y_1 \oplus Y_2 \oplus Y_3 \oplus Y_4 \oplus Y_5 \oplus Y_6 \oplus Y_7 \oplus Y_8$$

Para X = 1 (hamming: 1) e Y = 30 com um bias de -28 temos:

$$Pr[X_8 \oplus Y_4 \oplus Y_5 \oplus Y_6 \oplus Y_7 = 1] = 0.609$$

$$K_8 = W_8 \oplus Y_4 \oplus Y_5 \oplus Y_6 \oplus Y_7 \oplus 1$$

3 Resultados

Foram executadas 4000000 interações para que o seguinte valor de chave fosse obtido:

$$K = \{7, 6, 11, 2\}$$