Kryptografie und -analyse, Übung 6

Henry Haustein

Lineare Kryptoanalyse

(a) für $n = 1$:

$$\begin{aligned}\mathbb{P}(X_1 = 0) &= \frac{1}{2} + 2^{1-1}\left(p_1 - \frac{1}{2}\right)\\ &= p_1\end{aligned}$$

für $n = 2$:

$$\begin{aligned}\mathbb{P}(X_1 \oplus X_2 = 0) &= \frac{1}{2} + 2^{2-1}\left(p_1 - \frac{1}{2}\right)\left(p_2 - \frac{1}{2}\right)\\ &= \frac{1}{2} + 2\left(p_1p_2 - \frac{1}{2}p_1 - \frac{1}{2}p_2 + \frac{1}{4}\right)\\ &= \frac{1}{2} + 2p_1p_2 - p_1 - p_2 + \frac{1}{2}\\ &= 2p_1p_2 - p_1 - p_2 + 1\end{aligned}$$

vgl. aus Vorlesung $\mathbb{P}(X_1 \oplus X_2 = 0) = p_1p_2 + (1 - p_1)(1 - p_2)$

(b) für $n = 1$:

$$\begin{aligned}\mathbb{P}(X_1 = 0) &= \frac{1}{2} + 2^{1-1} \cdot \varepsilon_1\\ &= \frac{1}{2} + \varepsilon_1\end{aligned}$$

für $n = 2$:

$$\mathbb{P}(X_1 \oplus X_2 = 0) = \frac{1}{2} + 2^{2-1} \cdot \varepsilon_1 \cdot \varepsilon_2$$

(c) Tabelle

x	$f(x)$	$x^{[1,4]}$	$f(x)^{[2,3]}$	$x^{[1]} \oplus x^{[4]}$	$f(x)^{[2]} \oplus f(x)^{[3]}$
0 = 0000	e = 1110	00	11	0	0
1 = 0001	4 = 0100	01	10	1	1
2 = 0010	d = 1101	00	10	0	1
3 = 0011	1 = 0001	01	00	1	0

4 = 0100	2 = 0010	00	01	0	1
5 = 0101	f = 1111	01	11	1	0
6 = 0110	b = 1011	00	01	0	1
7 = 0111	8 = 1000	01	00	1	0
8 = 1000	3 = 0011	10	01	1	1
9 = 1001	a = 1010	11	01	0	1
a = 1010	6 = 0110	10	11	1	0
b = 1011	c = 1100	11	10	0	1
c = 1100	5 = 0101	10	10	1	1
d = 1101	9 = 1001	11	00	0	0
e = 1110	0 = 0000	10	00	1	0
f = 1111	7 = 0111	11	11	0	0

$\Rightarrow$ 6 Übereinstimmungen $\Rightarrow \frac{6}{16} = 0.375$. Das ist schlechter als Raten, es bietet sich hier an, eine affine lineare Approximation zu nutzen, indem man $f(x)^{[2,3]} = x^{[1,4]} \oplus 1$ nutzt. Die Güte ist dann $\frac{10}{16}$.

(d) Es gilt:

- $m_r = x_1$
- $m_l = y_1 \oplus x_2$
- $c_r = x_5$
- $c_l = y_5 \oplus x_4$
- $x_3 = m_r \oplus y_2 = c_r \oplus y_4$

Einsetzen in Approximationsgleichung für Runde 2:

$$\begin{aligned} k_2^{[26]} &= x_2^{[17]} \oplus y_2^{[3,8,14,25]} \oplus 1 \\ &= m_l^{[17]} \oplus y_1^{[17]} \oplus x_3^{[3,8,14,25]} \oplus m_r^{[3,8,14,25]} \oplus 1 \end{aligned}$$

Approximationsgleichung für Runde 4:

$$\begin{aligned} k_4^{[26]} &= x_4^{[17]} \oplus y_4^{[3,8,14,25]} \oplus 1 \\ &= c_l^{[17]} \oplus y_5^{[17]} \oplus x_3^{[3,8,14,25]} \oplus c_r^{[3,8,14,25]} \oplus 1 \end{aligned}$$

Approximationsgleichung für Runde 1:

$$\begin{aligned} k_1^{[2,3,5,6]} &= x_1^{[1,2,4,5]} \oplus y_1^{[17]} \oplus 1 \\ &= m_r^{[1,2,4,5]} \oplus y_1^{[17]} \oplus 1 \end{aligned}$$

Approximationsgleichung für Runde 5:

$$\begin{aligned} k_5^{[2,3,5,6]} &= x_5^{[1,2,4,5]} \oplus y_5^{[17]} \oplus 1 \\ &= c_r^{[1,2,4,5]} \oplus y_5^{[17]} \oplus 1 \end{aligned}$$

Addition der 4 Gleichungen liefert (Aufhebung von z.B. $y_1^{[17]} \oplus y_1^{[17]} = 0$)

$$\begin{aligned} k_1^{[2,3,5,6]} \oplus k_2^{[26]} \oplus k_4^{[26]} \oplus k_5^{[2,3,5,6]} &= m_r^{[1,2,4,5]} \oplus m_l^{[17]} \oplus m_r^{[3,8,14,25]} \oplus c_l^{[17]} \oplus c_r^{[3,8,14,25]} \oplus c_r^{[1,2,4,5]} \\ &= m_l^{[17]} \oplus m_r^{[1,2,3,4,5,8,14,15]} \oplus c_l^{[17]} \oplus c_r^{[1,2,3,4,5,8,14,15]} \\ &= m^{[17,33,34,35,36,37,40,46,57]} \oplus c^{[17,33,34,35,36,37,40,46,57]} \end{aligned}$$

Güte der Approximation mit Pilling-up-Lemma mit $n = 4$: $\frac{1}{2} + 2^3 \left(\frac{52}{64} - \frac{32}{64}\right)^2 \cdot \left(\frac{42}{64} - \frac{32}{64}\right)^2 = 0.519$