Kryptografie und -analyse, Übung 5

Henry Haustein

Differentielle Kryptoanalyse

(a) $S1_I^* = S1_I \oplus S1'_I = 110110 \oplus 011011 = 101101$
$S1_O = S1_2(110110) = 0111$, $S1_O^* = S1_3(101101) = 0001$
$S1'_O = 0111 \oplus 0001 = 0110$

(b) $S1'_E = 010001 \oplus 010010 = 000011$. Von den 64 möglichen Inputpaaren brauchen wir diejenigen, die Inputdifferenz von 3_{16} und Outputdifferenz 9_{16} haben. Dazu schauen wir in der Verteilungstabelle in der Spalte 9 nach Einsen. Es gibt 4 Inputpaare: (4,7), (7,4), (31,32), (32,31).
$S1_K = S1_I \oplus S1_E$

$S1_I$, $S1_I^*$	Schlüsselkandidaten
4, 7	15, 16
31, 32	20, 23

$\Rightarrow$ gesuchter Schlüssel ist 23
$\Rightarrow$ Differenz zwischen den Schlüsselkandidaten ist die Inputdifferenz der Eingaben. Mit immer derselben Differenz ist es nicht möglich einen eindeutigen Schlüssel zu erhalten.

(c) Da die Wahrscheinlichkeit der Charakteristik auch von den anderen S-Boxen abhängt, müssen die Wahrscheinlichkeiten der anderen S-Boxen möglichst groß sein (exakt 1). Da die S-Boxen deterministisch arbeiten, müssen die anderen S-Boxen eine Inputdifferenz von 0 verarbeiten. Die äußeren Bits sind für die Wahl der S-Box zuständig, deswegen dürfen nur die mittleren Bits von $S2'_I \neq 0$ ($\Rightarrow$ nur S2 aktiv). Damit ergeben sich folgende möglichen Inputdifferenzen:

- $000100 = 04 \Rightarrow$ Outputdifferenz 7 $\left(\frac{14}{64}\right)$
- $001000 = 08 \Rightarrow$ Outputdifferenz A $\left(\frac{16}{64}\right)$
- $001100 = 0C \Rightarrow$ Outputdifferenz 5 $\left(\frac{14}{64}\right)$

größte Wahrscheinlichkeit für $08 \to$ A mit $p = \frac{16}{64} = \frac{1}{4}$. 001000 sah vor der Expansion so aus: 0100. Alle anderen 4er-Blöcke sind 0. Damit $x' = 04000000_{16}$. Die Wahrscheinlichkeit für diese 1-Runden-Charakteristik ist damit:

$$\underbrace{1}_{S1} \cdot \underbrace{\frac{1}{4}}_{S2} \cdot \underbrace{1 \cdots 1}_{S3-S8} = \frac{1}{4}$$

$S2'_O = A \Rightarrow S1'_O\, S2'_O\, S3'_O\, ... = 0000\,1010\,0000...$ nach der Permutation werden die Einsen auf Position 5 und 7 auf die Positionen 13 und 2 permutiert. Alle anderen Bits sind 0. Damit ist $y' = 40080000$.

(d) Die Wahrscheinlichkeit für diese Charakteristik ist $p_1^\Omega \cdot p_2^\Omega$. Die Charakteristik ist so konstruiert, dass $p_1^\Omega = 1$ ist. Mit $L_{\Omega m} = 19600000$ sind die Inputdifferenzen für die S-Boxen (die Charakteristik ist so definiert, dass $S'_O = 0$ ist):

- Umwandlung in Binärdarstellung: 0001 1001 0110 0000 0000 0000 0000 0000
- Expansion: 000011 110010 101100 000000 000000 000000 000000 000000

Inputdifferenzen mit Wahrscheinlichkeiten

- $S1'_I = 3 \Rightarrow S1'_O = 0 \left(p = \frac{14}{64}\right)$
- $S2'_I = 32 \Rightarrow S2'_O = 0 \left(p = \frac{8}{64}\right)$
- $S3'_I = 2C \Rightarrow S3'_O = 0 \left(p = \frac{10}{64}\right)$
- $S4'_I = 0 \Rightarrow S4'_O = 0 \,(p = 1)$
- $S5'_I = 0 \Rightarrow S5'_O = 0 \,(p = 1)$
- $S6'_I = 0 \Rightarrow S6'_O = 0 \,(p = 1)$
- $S7'_I = 0 \Rightarrow S7'_O = 0 \,(p = 1)$
- $S8'_I = 0 \Rightarrow S8'_O = 0 \,(p = 1)$

$\Rightarrow p_2^\Omega = \frac{14}{64} \cdot \frac{8}{64} \cdot \frac{10}{64} \cdot 1 \cdots 1 = \frac{35}{8192}$ und somit $p^\Omega = p_1^\Omega \cdot p_2^\Omega = \frac{35}{8192}$.

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