E. Best

14.05.2004
Abgabe: 21.05.2004
Freitags in der Vorlesung

5. Übung zur Vorlesung Kryptographie

Achtung: Nächste Woche gibt es 2 Übungsgruppentermine:
Montag, 17.5., wie gewohnt; **Mittwoch**, 19.5., 8:15 in Raum A7-0-025.

Aufgabe 17: Wahrscheinlichkeiten und Bias (3+3+4 Punkte)

(a) Bestimmen Sie für das in der Vorlesung (S. 39) angegebene Beispiel für $x \in \{2, \ldots, 12\}$ und $y \in \{\text{NichtPasch}, \text{Pasch}\}$ alle Wahrscheinlichkeiten $\mathcal{P}[x, y]$, $\mathcal{P}[x|y]$ und $\mathcal{P}[y|x]$.

(b) Seien $\mathcal{X}_1$, $\mathcal{X}_2$ und $\mathcal{X}_3$ unabhängige diskrete Zufallsvariablen über $\{0, 1\}$. Sei ϵ_i der Bias von $\mathcal{X}_i$ $(1 \leq i \leq 3)$. Zeigen Sie, dass $\mathcal{X}_1 \circledast \mathcal{X}_2$ und $\mathcal{X}_2 \circledast \mathcal{X}_3$ genau dann unabhängig sind, wenn $\epsilon_1 = 0$, $\epsilon_3 = 0$ oder $|\epsilon_2| = \frac{1}{2}$.

(c) Berechnen Sie den Bias der Zufallsvariablen $\mathcal{X}_2 \circledast \mathcal{Y}_1 \circledast \mathcal{Y}_2 \circledast \mathcal{Y}_3 \circledast \mathcal{Y}_4$ für jede der acht DES-S-Boxen (Abb. 3.7). Dabei beziehen sich $\mathcal{X}_2$ auf das 2. Bit der Eingabe, $\mathcal{Y}_1, \mathcal{Y}_2, \mathcal{Y}_3, \mathcal{Y}_4$ auf die vier Bits der Ausgabe einer S-Box. [Zusatzbemerkung: diese Verzerrungen liegen relativ weit von $\frac{1}{2}$.]

Aufgabe 18: Lineare Attacke (4+4[+10] Punkte)

Wir nehmen an, dass die S-Box π_S im Beispiel des Abschnitts 3.2 ersetzt wird durch π'_S:

k	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi'_S(k)$	8	4	2	1	C	6	3	D	A	5	E	7	F	B	9	0

(a) Betrachten Sie die Zufallsvariable $\mathcal{X}_{16} \circledast \mathcal{U}_1^4 \circledast \mathcal{U}_9^4$. Finden Sie eine lineare Approximation mit möglichst wenigen relevanten S-Boxen und approximieren Sie nach dem Piling-Up-Lemma den Bias von $\mathcal{X}_{16} \circledast \mathcal{U}_1^4 \circledast \mathcal{U}_9^4$. Berechnen Sie dazu die (oder relevante Teile der) Tabelle der N_L-Werte für π'_S.

(b) Beschreiben Sie eine lineare Attacke (nach dem Muster des Algorithmus in Abbildung 3.5), der acht Schlüsselbits in der letzten Runde findet.

(c) **Bonusaufgabe (10 Extrapunkte):** Implementieren Sie Ihre Attacke und testen Sie sie, um zu sehen, wie viele Klartexte man ungefähr benötigt, um die korrekten Bits herauszufinden. (Hinweis: diese Attacke ist effizienter als die im Skript angegebene, weil die Verzerrungen höher sind.)

Aufgabe 19: Linearität bei S-Boxen im DES (2 Punkte)

Zeigen Sie, dass die DES-S-Box S_4 nicht linear ist. (Dabei gilt das exklusive oder $\circledast$ als $+$.)