Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Stefan Hoffmann, Ilya Ozerov

Hausübungen zur Vorlesung

Kryptographie

WS 2013/14

Blatt 3 / 28. Oktober 2013

Abgabe: 05. November 2013, 14.00 Uhr (vor der Vorlesung), Kasten NA/02

AUFGABE 1 (5 Punkte)**:**

Beweisen Sie „Komposition vernachlässigbarer Funktionen" auf Folie 27:

Seien $f_1(n), f_2(n)$ zwei vernachlässigbare Funktionen. Zeigen Sie:

(a) $f_1(n) + f_2(n)$ ist vernachlässigbar,

(b) $q(n) \cdot f_1(n)$ ist für ein beliebiges Polynom $q(n) \geq 0$ vernachlässigbar.

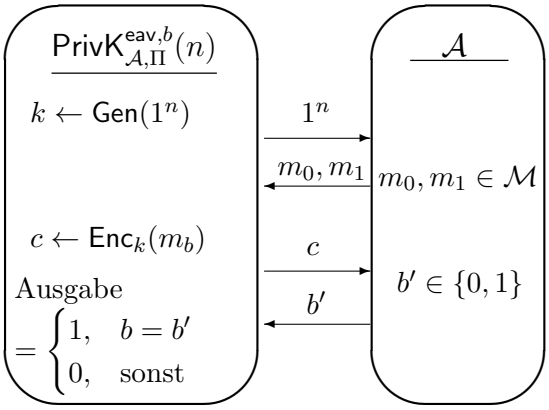
AUFGABE 2 (5 Punkte)**:**

Betrachten Sie ein symmetrisches Verschlüsselungsverfahren $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ mit Nachrichtenraum $\mathcal{M} = \{0,1\}^n$. Die *Paritätsfunktion* $\mathsf{parity} : \{0,1\}^n \to \{0,1\}$ sei definiert als $\mathsf{parity}(x) = \sum_i x_i \bmod 2$. Sei $\mathcal{A}$ ein ppt Algorithmus mit

$$\mathsf{Ws}[\mathcal{A}(1^n, \mathsf{Enc}_k(m)) = 1 - \mathsf{parity}(m)] = \frac{1}{3},$$

wobei die Wahrscheinlichkeit über die Wahl von $k \leftarrow \mathsf{Gen}(1^n)$, $m \in_R \mathcal{M}$, sowie die interne Randomisierung von $\mathcal{A}$ und Enc gebildet wird. Zeigen Sie, dass Π nicht KPA-sicher ist, indem Sie einen KPA-Angreifer $\mathcal{A}'$ konstruieren, der $\mathcal{A}$ benutzt.

Bitte wenden!



Betrachten Sie für die nächsten beiden Aufgaben erneut die Definitionen 1 und 2 der KPA-Sicherheit auf Präsenzblatt 3. Wir wollen nun eine dritte Definition beschreiben, für die wir das KPA-Spiel leicht modifizieren (siehe Abbildung oben).

Wir definieren dazu $\mathsf{PrivK}^{\mathsf{eav},b}_{\mathcal{A},\Pi}(n)$ für $b \in \{0,1\}$ analog zum KPA-Spiel, mit dem einzigen Unterschied, dass der Index der ausgewählten Nachricht, also das Bit b, nicht zufällig gewählt, sondern von außen fixiert wird. Das Ziel des Angreifers $\mathcal{A}$ ist nun zu entscheiden, in welchem Spiel $b = 0$ oder $b = 1$ er sich befindet. Die Ausgabe des Angreifers $\mathcal{A}$ wird im jeweiligen Spiel mit $b' = \mathsf{out}(\mathsf{PrivK}^{\mathsf{eav},b}_{\mathcal{A},\Pi}(n))$ bezeichnet.

Definition 3. Ein Verschlüsselungsschema $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ besitzt *ununterscheidbare Chiffretexte gegenüber KPA*, falls für alle ppt Angreifer $\mathcal{A}$ gilt

$$\left|\mathsf{Ws}[\mathsf{out}(\mathsf{PrivK}^{\mathsf{eav},1}_{\mathcal{A},\Pi}(n)) = 1] - \mathsf{Ws}[\mathsf{out}(\mathsf{PrivK}^{\mathsf{eav},0}_{\mathcal{A},\Pi}(n)) = 1]\right| \leq \mathsf{negl}(n)$$

AUFGABE 3 (5 Punkte)**:**

Zeigen Sie:

$$\mathsf{Ws}[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1] = \frac{1}{2} + \frac{1}{2} \cdot \left(\mathsf{Ws}[\mathsf{out}(\mathsf{PrivK}^{\mathsf{eav},1}_{\mathcal{A},\Pi}(n)) = 1] - \mathsf{Ws}[\mathsf{out}(\mathsf{PrivK}^{\mathsf{eav},0}_{\mathcal{A},\Pi}(n)) = 1]\right)$$

Hinweis: Begründen Sie, dass $\mathsf{Ws}[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1 \mid b = j] = \mathsf{Ws}[\mathsf{PrivK}^{\mathsf{eav},j}_{\mathcal{A},\Pi}(n) = 1]$ und $\mathsf{Ws}[\mathsf{PrivK}^{\mathsf{eav},j}_{\mathcal{A},\Pi}(n) = 1] = \mathsf{Ws}[\mathsf{out}(\mathsf{PrivK}^{\mathsf{eav},j}_{\mathcal{A},\Pi}(n)) = j]$ für $j \in \{0,1\}$ gilt.

AUFGABE 4 (5 Punkte)**:**

Zeigen Sie in dieser Aufgabe die Äquivalenz der drei Definitionen der KPA-Sicherheit. In Aufgabe 4 der Präsenzübung wurde bereits gezeigt, dass die erste Definition die zweite Definition impliziert. Zeigen Sie für einen Ringschluss:

(a) Definition 2 impliziert Definition 3,

(b) Definition 3 impliziert Definition 1.

Hinweis: Verwenden Sie Aufgabe 3.