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

Hausübungen zur Vorlesung

Kryptographie

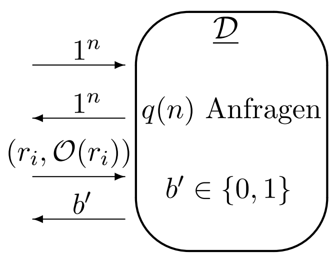
WS 2013/14

Blatt 5 / 12. November 2013 (Update!)

Abgabe: 19. November 2013, 14.00 Uhr (vor der Vorlesung), Kasten NA/02

AUFGABE 1 (8 Punkte)**:**

Für ein Orakel $\mathcal{O} : \{0,1\}^n \to \{0,1\}^n$ sei $\mathcal{O}^R(\cdot)$ ein Orakel, das bei Eingabe 1^n gleichverteilt ein $r \in_R \{0,1\}^n$ wählt und $(r, \mathcal{O}(r))$ zurückgibt. Im Vergleich zu einem gewöhnlichen Orakel hat man nun also keine Kontrolle mehr über die Eingabe und das Spiel ändert sich wie folgt.



Wir bezeichnen eine schlüsselabhängige Funktion $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ als *schwache Pseudozufallsfunktion*, falls für alle ppt-Algorithmen $\mathcal{D}$

$$\left| \mathsf{Ws}[\mathcal{D}^{F_k^R(\cdot)}(1^n) = 1] - \mathsf{Ws}[\mathcal{D}^{f^R(\cdot)}(1^n) = 1] \right| \leq \mathsf{negl}(n),$$

wobei $k \in_R \{0,1\}^n$ und $f \in_R \mathsf{Func}_n$ gleichverteilt gewählt werden.

Sei $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ eine Pseudozufallsfunktion. Wir definieren eine neue Funktion $F' : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ als $F'_k(x) := F_k(x \wedge 1^{n-1}0)$, d.h. das letzte Bit der Eingabe wird stets auf 0 gesetzt und dann F_k aufgerufen.

(a) Zeigen Sie, dass F' eine *schwache Pseudozufallsfunktion* ist.

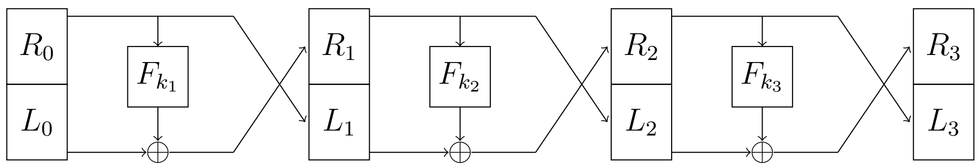
(b) Zeigen Sie, dass F' <u>keine</u> *Pseudozufallsfunktion* ist.

Bitte wenden!

AUFGABE 2 (6 Punkte)**:**

Sei $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ eine Pseudozufallsfunktion. Wir konstruieren aus F eine Permutation $F' : \{0,1\}^{3n} \times \{0,1\}^{2n} \to \{0,1\}^{2n}$, die wie unten abgebildet (Feistelnetzwerk mit 3 Runden) aus der Eingabe (L_0, R_0) die Ausgabe (L_3, R_3) berechnet, wobei $k_1, k_2, k_3 \in \{0,1\}^n$ der erste, zweite, bzw. dritte Teil des Schlüssels k von F' ist. Es gilt also

$$L_i = R_{i-1} \text{ und } R_i = L_{i-1} \oplus F_{k_i}(R_{i-1}).$$

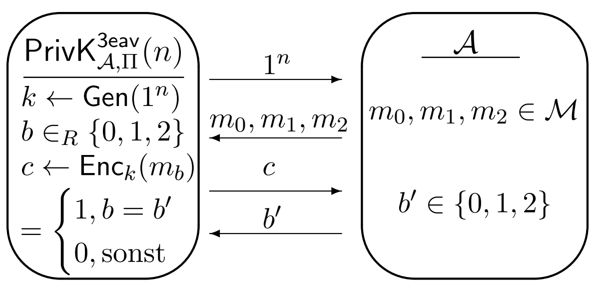


Zeigen Sie, dass F' <u>keine</u> *starke* Pseudozufallspermutation ist.

Hinweis: Stellen Sie eine Anfrage an $\mathcal{O}$, eine an $\mathcal{O}^{-1}$ und schließlich wieder eine an $\mathcal{O}$.

AUFGABE 3 (6 Punkte)**:**

In dieser Aufgabe wollen wir uns eine Alternative zur in der Vorlesung definierten KPA-Sicherheit anschauen. Dabei ist der einzige Unterschied, dass der Angreifer $\mathcal{A}$ drei statt zwei Nachrichten wählen muss, von denen dann auch hier eine (aus den dreien uniform gewählte) verschlüsselt wird.



Sei $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ ein symmetrisches Verschlüsselungsverfahren mit $|\mathcal{M}| \geq 3$. Π heißt 3KPA-sicher, falls für alle ppt-Angreifer $\mathcal{A}$

$$\mathsf{Ws}[\mathsf{PrivK}^{\mathsf{3eav}}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{3} + \mathsf{negl}(n).$$

Sei $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ ein symmetrisches Verschlüsselungsverfahren mit $|\mathcal{M}| \geq 3$. Zeigen Sie, dass Π 3KPA-sicher ist, falls Π KPA-sicher ist.

Hinweis: Konstruieren Sie einen Angreifer auf die KPA-Sicherheit von Π, der aus den drei Nachrichten des 3KPA-Angreifers uniform eine *nicht* weiterschickt. Sie müssen dann zeigen, dass der 3KPA-Angreifer auf diese Weise die Verschlüsselung einer (aus seinen drei geschickten) uniform gewählten Nachricht erhält. Sie dürfen für den Beweis davon ausgehen, dass der 3KPA-Angreifer stets paarweise verschiedene Nachrichten wählt.