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

Präsenzübungen zur Vorlesung

Kryptographie I

WS 2012/13

Blatt 4 / 26./28. November 2012

AUFGABE 1:

Betrachten Sie die folgende längenerhaltende, schlüsselabhängige Funktion F mit $F_A : \{0,1\}^n \to \{0,1\}^n$, wobei $A \in_R \{0,1\}^{n \times n}$:

$$F_A(m) := A \cdot m \quad \text{(Matrix-Vektor-Produkt)}.$$

Zeigen Sie, dass F keine Pseudozufallsfunktion ist.

AUFGABE 2:

Ist es möglich eine Pseudozufallsfunktion $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ aus einem Pseudozufallsgenerator $G : \{0,1\}^n \to \{0,1\}^{n+1}$ zu konstruieren?

◯ **JA**
◯ **NEIN**

AUFGABE 3:

Für eine Funktion $g : \{0,1\}^n \to \{0,1\}^n$ sei $g^R(\cdot)$ ein Orakel, das bei Eingabe 1^n gleichverteilt ein $r \in_R \{0,1\}^n$ wählt und $(r, g(r))$ zurückgibt. Im Vergleich zu einem gewöhnlichen Orakel hat man nun also keine Kontrolle mehr über die Eingabe. Wir bezeichnen eine schlüsselabhängige Funktion F 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.

Zeigen Sie, dass jede Pseudozufallsfunktion auch eine *schwache Pseudozufallsfunktion* ist.

AUFGABE 4:

Beweisen Sie, dass jede Pseudozufallspermutation eine Pseudozufallsfunktion ist (siehe Satz auf Folie 82). Gehen Sie wie folgt vor:

(a) Begründen Sie, warum es ausreicht zu zeigen, dass kein Unterscheider $\mathcal{D}$ eine echte Zufallsfunktion $f \in_R \mathsf{Func}_n$ von einer echten Zufallspermutation $g \in_R \mathsf{Perm}_n$ unterscheiden kann, d.h.

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

(b) Zeigen Sie (1). Hierfür kann es hilfreich sein, ein Ereignis Coll zu betrachten, dass $\mathcal{D}$ zwei Werte $x \neq y$ mit $\mathcal{O}(x) = \mathcal{O}(y)$ bei seinem Orakel $\mathcal{O}$ anfragt. Benutzen Sie dann, dass Coll höchstens mit Wahrscheinlichkeit $\frac{q(n)^2}{2^n}$ auftritt, wenn $\mathcal{O}(\cdot) = f(\cdot)$ ist und $q(n)$ die Anzahl der Orakelanfragen bezeichnet. Was passiert für $\mathcal{O}(\cdot) = g(\cdot)$?