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 6 / 15. November 2013

Abgabe: 26. November 2013, 14.00 Uhr (vor der Vorlesung), Kasten NA/02

AUFGABE 1 (5 Punkte)**:**

Sei $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ eine Pseudozufallsfunktion. Betrachten Sie folgende Variante $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ des Counter Modes:

$\mathsf{Gen}(1^n)$: Wähle $k \in_R \{0,1\}^n$ und $\mathcal{S} \subset \{0,1\}^n$ mit $|\mathcal{S}| = p(n)$ für ein Polynom $p(n) > 0$.

$\mathsf{Enc}_{k,\mathcal{S}}(m)$: Wähle $\mathsf{IV} \in_R \mathcal{S}$, $r_i := F_k(\mathsf{IV} + i - 1 \bmod 2^n)$, $c_i := r_i \oplus m_i$, $1 \leq i \leq \ell$.
Ausgabe $c := (\mathsf{IV}, c_1, \ldots, c_\ell)$.

Zeigen Sie, dass Π nicht CPA-sicher ist.

AUFGABE 2 (5 Punkte)**:**

Sei $n \in \mathbb{N}$ gerade und $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ eine Pseudozufallspermutation. Wir konstruieren aus F ein symmetrisches Verschlüsselungsverfahren $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ mit Nachrichtenraum $\mathcal{M} = \{0,1\}^{n/2}$ und

$\mathsf{Gen}(1^n)$: Gib $k \in_R \{0,1\}^n$ zurück.

$\mathsf{Enc}_k(m)$: Wähle $r_1, r_2 \in_R \{0,1\}^{n/2}$ und gib $c := (r_1, r_2, F_k(m, r_1 \oplus r_2))$ zurück.

$\mathsf{Dec}_k(c)$: Für $c = (c_1, c_2, c_3)$ berechne $(x_1, x_2) := F_k^{-1}(c_3)$ mit $x_1, x_2 \in \{0,1\}^{n/2}$ und gib zurück:

$$m := \begin{cases} x_1 & , \text{falls } c_1 \oplus c_2 = x_2 \\ \perp & , \text{sonst} \end{cases}$$

Zeigen Sie, dass Π nicht CCA-sicher ist.

Bitte wenden!

AUFGABE 3 (5 Punkte)**:**

Sei $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ eine schlüsselabhängige Funktion. Betrachten Sie die Konstruktion $\Pi_B = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ aus der Vorlesung mit $\mathcal{M} = \{0,1\}^n$ und

$\mathsf{Gen}(1^n)$: Gib $k \in_R \{0,1\}^n$ zurück.

$\mathsf{Enc}_k(m)$: Wähle $r \in_R \{0,1\}^n$ und gib $c := (r, F_k(r) \oplus m)$ zurück.

$\mathsf{Dec}_k(c)$: Für $c = (c_1, c_2)$ gib $m := F_k(c_1) \oplus c_2$ zurück.

Zeigen Sie, dass F eine *schwache* Pseudozufallsfunktion ist, falls Π_B CPA-sicher ist.

Hinweis: Verwenden Sie die Eigenschaft, dass jedes CPA-sichere Verschlüsselungsverfahren auch mult-CPA-sicher ist. Nehmen Sie o.B.d.A. zudem an, dass Sie wissen, wie viele Anfragen der Unterscheider für F (maximal) stellen wird (da die Anzahl ein Polynom ist, kann man sie immer raten).

AUFGABE 4 (5 Punkte)**:**

Sei $n \in \mathbb{N}$ gerade und $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ eine schlüsselabhängige Permutation. Wir konstruieren aus F ein symmetrisches Verschlüsselungsverfahren $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ mit Nachrichtenraum $\mathcal{M} = \{0,1\}^{n/2}$ und

$\mathsf{Gen}(1^n)$: Gib $k \in_R \{0,1\}^n$ zurück.

$\mathsf{Enc}_k(m)$: Wähle $r \in_R \{0,1\}^{n/2}$ und gib $c := F_k(r, m)$ zurück.

(a) Geben Sie einen Entschlüsselungsalgorithmus an und zeigen Sie die Korrektheit.

(b) Zeigen Sie, dass Π CPA-sicher ist, falls F eine Pseudozufallspermutation ist.