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

Präsenzübungen zur Vorlesung

Kryptographie I

WS 2012/13

Blatt 5 / 10./12. Dezember 2012

AUFGABE 1:

Ist der Counter-Modus CPA-sicher, falls (statt einer Pseudozufallsfunktion) eine *schwache Pseudozufallsfunktion* verwendet wird? Der Counter-Modus ist für ein $\ell \in \mathbb{N}$ und Nachrichtenraum $\mathcal{M} = \{0,1\}^{n\ell}$ definiert als $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ mit:

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

$\mathsf{Enc}_k(m)$: $\mathsf{IV} \in_R \{0,1\}^n$, $c_i := m_i \oplus F_k(\mathsf{IV} + i - 1 \bmod 2^n)$ für $1 \leq i \leq \ell$, $c := (\mathsf{IV}, c_1, \ldots, c_\ell)$.

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. 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.

AUFGABE 2:

Betrachten Sie eine Variante des CBC Modus, in der der Initialisierungsvektor nur polynomiell viele Werte annehmen kann, d.h. $\mathsf{IV} \in_R \mathcal{S}$ für ein $\mathcal{S} \subset \{0,1\}^n$ mit $|\mathcal{S}| = p(n)$ für ein Polynom $p(n) > 0$. Ist der CBC Modus dann noch CPA-sicher?

AUFGABE 3:

Sei $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ eine Pseudozufallsfunktion. Betrachten Sie den folgenden MAC $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ für Nachrichten $m \in \{0,1\}^{2n}$ fester Länge.

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

$\mathsf{Mac}_k(m)$: Berechnet für eine Nachricht $m = (m_0, m_1)$ mit $|m_0| = |m_1| = n$ den Tag

$$t := (F_k(m_0), F_k(F_k(m_1))).$$

Geben Sie eine korrekte Vrfy-Funktion an. Ist der MAC sicher?