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 7 / 22. November 2013

Abgabe: 03. Dezember 2013, 14.00 Uhr (vor der Vorlesung), Kasten NA/02

AUFGABE 1 (5 Punkte)**:**

Sei $\Pi' = (\mathsf{Gen}', \mathsf{Mac}', \mathsf{Vrfy}')$ ein sicherer MAC für Nachrichten der festen Länge $4n$. Betrachten Sie den folgenden MAC $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ für Nachrichten der festen Länge $6n$:

$\mathsf{Gen}(1^n)$: Gib $k \leftarrow \mathsf{Gen}'(1^n)$ zurück.

$\mathsf{Mac}_k(m)$: Für $m = (m_0, m_1)$ mit $m_i \in \{0,1\}^{3n}$ wähle $r \in_R \{0,1\}^{n-1}$ und gib zurück:

$$t := (r, t_0, t_1) := (r, \mathsf{Mac}'_k(m_0, 0, r), \mathsf{Mac}'_k(m_1, 1, r))$$

$\mathsf{Vrfy}_k(m,t)$: Für $(m,t) = (m_0, m_1, r, t_0, t_1)$ gib zurück:

$$\begin{cases} 1, & \mathsf{Vrfy}'_k((m_0,0,r),t_0) = 1 \text{ und } \mathsf{Vrfy}'_k((m_1,1,r),t_1) = 1 \\ 0, & \text{sonst} \end{cases}$$

Zeigen Sie, dass Π sicher ist.

Hinweis: Orientieren Sie sich an dem Π_{MAC2} Beweis aus der Vorlesung (Folie 110 ff.).

AUFGABE 2 (5 Punkte)**:**

Sei $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ ein MAC mit Nachrichten, Tags und Schlüsseln aus $\{0,1\}^n$,

$$\mathsf{Mac}_k(\mathsf{Mac}_k(m)) = m, \quad \text{aber} \quad \mathsf{Mac}_k(m) \neq m$$

für alle $m, k \in \{0,1\}^n$.

Zeigen Sie, dass Π kein sicherer MAC ist.

Bitte wenden!

AUFGABE 3 (5 Punkte)**:**

Sei $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ eine Pseudozufallsfunktion. Betrachten Sie eine Variante $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ des CBC-MAC aus der Vorlesung (Folie 117) für *variable* Nachrichtenlänge:

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

$\mathsf{Mac}_k(m)$: Für $k \in \{0,1\}^n$ und $m = m_1, \ldots, m_\ell \in (\{0,1\}^n)^\ell$ setze $t_0 := 0^n$,

$$t_i := F_k(t_{i-1} \oplus m_i) \text{ für } i = 1, \ldots, \ell$$

und $t_{\ell+1} := F_k(t_\ell \oplus \ell)$, wobei $\ell \in \{0,1\}^n$ kodiert wird. Gib $t := t_{\ell+1}$ zurück.

In dieser Variante wird die Länge der Nachricht folglich *hinten* angehangen.

(a) Geben Sie eine korrekte Vrfy-Funktion an.

(b) Zeigen Sie, dass Π nicht sicher ist.

Hinweis: Aufgabenteil (b) lässt sich mit zwei Anfragen lösen. Nutzen Sie aus, dass Nachrichten unterschiedlicher Länge ℓ angefragt werden dürfen.

AUFGABE 4 (5 Punkte)**:**

Sei (Gen, H) eine kollisionsresistente Hashfunktion. Betrachten Sie nun die Hashfunktion $(\mathsf{Gen}, \hat{H})$ mit $\hat{H}_s(x) := H_s(H_s(x))$.

Ist die neue Hashfunktion kollisionsresistent? Falls ja, geben Sie eine Reduktion an, die aus einer Kollision in $\hat{H}$ eine Kollision in H bestimmt. Falls nein, geben Sie einen Angreifer an, der eine Kollision in $\hat{H}$ berechnet.