Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Alexander Meurer, Florian Giesen

Hausübungen zur Vorlesung

Kryptographie 1

WS 2010/11

Blatt 7 / 24. Januar 2011 / Abgabe 7. Februar, 16 Uhr, Kasten NA 02

Im Satz zur Sicherheit des NMAC (Folie 132) benötigt man zwei Annahmen, nämlich die Kollisionsresistenz der Kompressionsfunktion $\Pi = (\mathsf{Gen}, h)$ *und* die Sicherheit des aus h abgeleiteten MACs Π_h fester Länge (siehe Folie 131). Wir wollen nun zeigen, dass die Sicherheit von Π_h im Allgemeinen *nicht* aus der Kollisionsresistenz von h folgt.

AUFGABE 1. NMAC. (5 Punkte)
Zeigen Sie, dass es eine kollisionsresistente Hashfunktion $\Pi = (\mathsf{Gen}, h)$ mit $h_s : \{0,1\}^{3\ell} \to \{0,1\}^{2\ell}$ gibt, so dass der daraus resultierende MAC Π_h *nicht* sicher ist. Gehen Sie hierbei wie folgt vor.

a) Sei $\widetilde{\Pi} = (\widetilde{\mathsf{Gen}}, g)$ mit $g_s : \{0,1\}^{2\ell} \to \{0,1\}^{\ell}$ eine kollisionsresistente Hashfunktion. Konstruieren Sie $\Pi = (\mathsf{Gen}, h)$ durch $h_s(x) := (x_1, g_s(x_2))$ mit $x_1 \in \{0,1\}^{\ell}$ und $x_2 \in \{0,1\}^{2\ell}$. Beweisen Sie, dass Π kollisionsresistent ist, indem Sie aus einem Angreifer $\mathcal{A}$ für Π einen Angreifer $\widetilde{\mathcal{A}}$ für $\widetilde{\Pi}$ konstruieren.

b) Zeigen Sie, dass Π_h mit h aus Teil a) *kein* sicherer MAC ist, indem Sie einen Algorithmus angeben, der Fälschungen berechnet. Gehen Sie hierbei davon aus, dass Π_h wie folgt auf die Eingabelänge 3ℓ von h_s angepasst wird: Wähle Schlüssel $k \in \{0,1\}^{\ell}$ und Nachrichten $m \in \{0,1\}^{2\ell}$ und berechne den Tag $t = h_s(k||m)$.

AUFGABE 2. Eindeutig zweideutig. (5 Punkte)
Geben Sie einen MAC $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ an, so dass die Konstruktion Π_{cca} (siehe Folie 139) *nicht* CCA-sicher ist. Beweisen Sie die Sicherheit des von Ihnen gewählten MACs Π und geben Sie einen CCA-Angreifer auf Π_{cca} an.

Hinweis: Geben Sie einen sicheren MAC Π an, welcher die Eigeschaft *eindeutige Tags* (Folie 140) verletzt. Diesen kann man bspw. aus einem sicheren MAC $\widetilde{\Pi} = (\widetilde{\mathsf{Gen}}, \widetilde{\mathsf{Mac}}, \widetilde{\mathsf{Vrfy}})$ konstruieren, indem man $\mathsf{Mac}_k(m) := (t, r)$ mit $t = \widetilde{\mathsf{Mac}}_k(m)$ und $r \in_R \{0,1\}$ definiert.

AUFGABE 3. CCA Sicherheit. (10 Punkte)
Es sei $F := \{F_k : \{0,1\}^{3n} \rightarrow \{0,1\}^{3n} | k \in \{0,1\}^n\}$ eine *starke* Pseudozufallspermutation (siehe Folie 153). Betrachten Sie das Verschlüsselungsverfahren $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ defniert als

- $\mathsf{Gen}(1^n)$ gibt zuälligen Schlüssel $k \in_R \{0,1\}^n$ aus.
- $\mathsf{Enc}_k(m)$ wählt Randomisierung $r \in_R \{0,1\}^n$ und gibt $c = F_k(r||m||0^n)$ aus.
- $\mathsf{Dec}_k(c)$ berechnet $(x_1, x_2, x_3) = \mathsf{Dec}_k(c)$ mit $x_i \in \{0,1\}^n$. Falls $x_3 = 0^n$ so gib x_2 aus, sonst gibt Fehlersymnol $\perp$ aus.

Zeigen Sie, dass Π CCA-sicher ist, indem Sie aus einem CCA-Angreifer $\mathcal{A}$ einen Unterscheider $\mathcal{D}$ für F konstruieren.

Hinweis: Überlegen Sie, wie man ähnlich zum Beweis der CCA-Sicherheit von Π_{cca} (siehe Folie 141) argumentieren kann, dass das Entschlüsselungsorakel nutzlos ist.