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

Präsenzübungen zur Vorlesung

Kryptographie I

WS 2012/13

Blatt 7 / 21./23. Januar 2013

AUFGABE 1:

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 den Schlüssel $k \in \{0,1\}^{\ell}$ und die Nachrichten $m \in \{0,1\}^{2\ell}$ und berechne den Tag $t := h_s(k, m)$.

AUFGABE 2:

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 Eigenschaft *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 $\mathsf{Mac}_k(m) := (\widetilde{\mathsf{Mac}}_k(m), r)$ mit $r \in_R \{0,1\}$ definiert.

AUFGABE 3:

Zeigen Sie, dass Π'_B nicht CCA-sicher ist.

Erinnerung: In Π'_B wird eine Pseudozufallsfunktion F verwendet. Eine Nachricht $m = m_1 \dots m_\ell$ mit $m_i \in \{0,1\}^n$ wird verschlüsselt, indem $r_1, \dots, r_\ell \in_R \{0,1\}^n$ gewählt werden und anschließend

$$c := (r_1, \dots, r_\ell, F_k(r_1) \oplus m_1, \dots, F_k(r_\ell) \oplus m_\ell)$$

ausgegeben wird.

AUFGABE 4:

Konstruieren Sie ein Verschlüsselungsverfahren $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$, welches CCA-sicher ist, aber keine *authentisierte Kommunikation* (siehe Folie 145) bietet. Zeigen Sie die CCA-Sicherheit Ihres Systems und geben Sie dann einen Angreifer im Auth-Spiel an.

Hinweis: Gehen Sie von einem CCA-sicheren Verfahren aus, und fügen Sie einen „künstlichen" Chiffretext für einen ausgezeichneten Klartext hinzu, welcher aber gar nicht von Enc ausgegeben wird.