



Präsenzübungen zur Vorlesung  
Kryptographie  
WS 2013/14  
Blatt 8 / 2./3. Dezember 2013

**AUFGABE 1:**

Zeigen Sie, dass es eine kollisionsresistente Hashfunktion  $\Pi = (\text{Gen}, h)$  mit  $h_s : \{0, 1\}^{3\ell} \rightarrow \{0, 1\}^{2\ell}$  gibt, so dass der daraus resultierende MAC  $\Pi_h$  nicht sicher ist. Gehen Sie hierbei wie folgt vor.

- Sei  $\tilde{\Pi} = (\widetilde{\text{Gen}}, g)$  mit  $g_s : \{0, 1\}^{2\ell} \rightarrow \{0, 1\}^\ell$  eine kollisionsresistente Hashfunktion. Konstruieren Sie  $\Pi = (\text{Gen}, h)$  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  $\Pi$  kollisionsresistent ist, indem Sie aus einem Angreifer  $\mathcal{A}$  für  $\Pi$  einen Angreifer  $\tilde{\mathcal{A}}$  für  $\tilde{\Pi}$  konstruieren.
- Zeigen Sie, dass  $\Pi_h$  mit  $h$  aus Teil (a) kein sicherer MAC ist, indem Sie einen Algorithmus angeben, der Fälschungen berechnet. Gehen Sie hierbei davon aus, dass  $\Pi_h$  wie folgt auf die Eingabelänge  $3\ell$  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  $\Pi = (\text{Gen}, \text{Mac}, \text{Vrfy})$  an, so dass die Konstruktion  $\Pi_{\text{cca}}$  (siehe Folie 141) nicht CCA-sicher ist. Beweisen Sie die Sicherheit des von Ihnen gewählten MACs  $\Pi$  und geben Sie einen CCA-Angreifer auf  $\Pi_{\text{cca}}$  an.

*Hinweis:* Geben Sie einen sicheren MAC  $\Pi$  an, welcher die Eigenschaft *eindeutige Tags* (Folie 142) verletzt. Diesen kann man bspw. aus einem sicheren MAC  $\tilde{\Pi} = (\widetilde{\text{Gen}}, \widetilde{\text{Mac}}, \widetilde{\text{Vrfy}})$  konstruieren, indem man  $\text{Mac}_k(m) := (\widetilde{\text{Mac}}_k(m), r)$  mit  $r \in_R \{0, 1\}$  definiert.

### AUFGABE 3:

Zeigen Sie, dass  $\Pi'_B$  nicht CCA-sicher ist.

*Erinnerung:* In  $\Pi'_B$  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  $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ , welches CCA-sicher ist, aber keine *authentisierte Kommunikation* (siehe Folie 147) 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.