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

RUHR UNIVERSITÄT BOCHUM RUB

Lösungsblatt 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 $t = h_s(k||m)$.

Lösungsvorschlag:

a) Sei $\mathcal{A}$ ein Angreifer für Π mit Vorteil $\epsilon_{\mathcal{A}}(n)$. Konstruiere $\widetilde{\mathcal{A}}$ für $\widetilde{\Pi}$ wie folgt:

- $\widetilde{\mathcal{A}}$ erhält Eingabe $(1^n, s)$ und ruft $\mathcal{A}(1^n, s)$ auf.
- $\mathcal{A}$ liefert x, x' mit $x = (x_1, x_2)$ und $x' = (x'_1, x'_2)$ mit $x_1, x'_1 \in \{0,1\}^{\ell}$ und $x_2, x'_2 \in \{0,1\}^{2\ell}$.
- $\widetilde{\mathcal{A}}$ gibt x_2, x'_2 aus.

Beachte, dass jede Kollision $x \neq x'$ für h_s die Bedingung $(x_1, g_s(x_2)) = h_s(x) = h_s(x') = (x'_1, g_s(x'_2))$ erfüllen muss. Wegen $x_1 = x'_1$ und $x \neq x'$ muss stets $x_2 \neq x'_2$ gelten. Außerdem

gilt offensichtlich $g_s(x_2) = g_s(x_2')$. Insgesamt kann also aus jeder Kollision x, x' für h_s die Kollision x_2, x_2' für g_s berechnet werden. Formal folgt hieraus

$$\begin{aligned}\epsilon_{\widetilde{\mathcal{A}}}(n) &= \mathbf{Ws}\left[\mathsf{HashColl}_{\widetilde{\mathcal{A}},\widetilde{\Pi}}(n) = 1\right] = \mathbf{Ws}\left[x_2 \neq x_2' \wedge g_s(x_2) = g_s(x_2')\right] \\ &\geq \mathbf{Ws}\left[x \neq x' \wedge h_s(x) = h_s(x')\right] = \mathbf{Ws}\left[\mathsf{HashColl}_{\mathcal{A},\Pi}(n) = 1\right] = \epsilon_{\mathcal{A}}(n) \ .\end{aligned}$$

Nach Voraussetzung ist $\widetilde{\Pi}$ kollisionsresistent und es folgt $\epsilon_{\mathcal{A}}(n) \leq \epsilon_{\widetilde{\mathcal{A}}}(n) = \mathsf{negl}(n)$. Somit ist auch Π kollisionsresistent.

b) Offenbar gibt ein einziger Tag $t = h_s(k||m) = (k, g_s(m))$ bereits den gesamten geheimen Schlüssel preis. Damit kann ein Angreifer nach einer einzigen Signieranfrage beliebige Fälschungen berechnen. Formaler betrachten wir folgenden Fälscher $\mathcal{F}$.

- $\mathcal{F}$ erhält $(1^n, s)$.
- $\mathcal{F}$ stellt eine Signieranfrage für die Nachricht $m = 0^{2\ell}$.
- $\mathcal{F}$ erhält einen gültigen Tag $t = (t_1, t_2) = h_s(k||m)$.
- $\mathcal{F}$ berechnet für die Nachricht $m^* = 1^{2\ell} \neq m$ den gültigen Tag $t^* = h_s(t_1||m^*)$ und gibt (t^*, m^*) aus.

Offenbar gilt $t_1 = k$ und somit gewinnt $\mathcal{F}$ sein Forge-Spiel mit Wahrscheinlichkeit 1.

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.

Lösungsvorschlag:

Zunächst konstruieren wir einen sicheren MAC Π mit *merhdeutigen* Tags aus einem MAC $\widetilde{\Pi}$ mit eindeutigen Tags wie folgt.

- $\mathsf{Gen}(1^n)$ gibt $k \leftarrow \widetilde{\mathsf{Gen}}(1^n)$ aus.
- $\mathsf{Mac}_k(m)$ berechnet $t = (\widetilde{t}, r)$ mit $\widetilde{t} = \widetilde{Mac}_k(m)$ und $r \in_R \{0,1\}$.
- $\mathsf{Vrfy}_k(m, (\widetilde{t}, r))$ gibt 1 aus genau dann, wenn $\widetilde{\mathsf{Vrfy}}_k(m, \widetilde{t}) = 1$.

Wir zeigen nun, dass Π sicher ist falls $\widetilde{\Pi}$ sicher ist. Sei hierzu $\mathcal{A}$ ein Angreifer für Π mit Vorteil $\epsilon_{\mathcal{A}}(n)$. Wir konstruieren einen Angreifer $\widetilde{\mathcal{A}}$ mittels $\mathcal{A}$ wie folgt.

- $\widetilde{\mathcal{A}}$ erhält 1^n und ruft $\mathcal{A}(1^n)$ auf.

- $\mathcal{A}$ stellt Signieranfragen m_i für $i \in [q]$ welche $\widetilde{\mathcal{A}}$ wie folgt beantwortet: $\widetilde{\mathcal{A}}$ fragt einen Tag $\widetilde{t}_i = \widetilde{\mathsf{Mac}}_k(m_i)$ an und sendet $t_i := (\widetilde{t}_i, r_i)$ für zufälliges $r_i \in_R \{0,1\}$ an $\mathcal{A}$.
- $\mathcal{A}$ sendet Fälschung (m^*, t^*) wobei $t^* = (\widetilde{t}^*, r^*)$ gilt.
- $\widetilde{\mathcal{A}}$ gibt die Fälschung $(m^*, \widetilde{t}^*)$ aus.

Beachte, dass eine *gültige* Fälschung (m^*, t^*) von $\mathcal{A}$ sowohl $m^* \neq m_i$ für alle $i \in [q]$ als auch $\widetilde{\mathsf{Vrfy}}_k(m^*, \widetilde{t}^*) = 1$ erfüllen muss, d.h. die Ausgabe $(m^*, \widetilde{t}^*)$ ist eine gültige Fälschung. Somit folgt

$$\begin{aligned}\epsilon_{\widetilde{A}}(n) &= \mathbf{Ws}\left[\mathsf{MacForge}_{\widetilde{\mathcal{A}},\widetilde{\Pi}}(n) = 1\right] \\ &= \mathbf{Ws}\left[m^* \neq m_i \wedge \widetilde{\mathsf{Vrfy}}_k(m^*, \widetilde{t}^*) = 1\right] = \mathbf{Ws}\left[\mathsf{MacForge}_{\mathcal{A},\Pi}(n) = 1\right] = \epsilon_{\mathcal{A}}(n) \ .\end{aligned}$$

Da $\widetilde{\Pi}$ nach Voraussetzung sicher ist, folgt $\epsilon_{\mathcal{A}}(n) = \epsilon_{\widetilde{\mathcal{A}}}(n) \leq \mathsf{negl}(n)$ und somit ist Π sicher.

Wir verwenden nun Π in der Konstruktion Π_{cca} aus der Vorlesung. Wir zeigen nun, dass Π_{cca} für diese Instantiierung von Π *nicht* CCA-sicher ist indem wir folgenden Angreifer $\mathcal{A}_{\text{cca}}$ betrachten. Es bezeichne

$$(c^*, t^*) = (\mathsf{Enc}_{k_1}(m_b), \mathsf{Mac}_{k_2}(c^*))$$

den Challenge-Ciphertext von $\mathcal{A}_{\text{cca}}$. Dann hat der Tag t^* nach obiger Konstruktion die Gestalt

$$t^* = (\widetilde{t}^*, r^*) = (\widetilde{\mathsf{Mac}}_{k_2}(c^*), r^*)$$

und $\mathcal{A}_{\text{cca}}$ kann leicht einen neuen gültigen Tag $t^{**} := (\widetilde{t}^*, \overline{r^*})$ mit $\overline{r^*} = r^* \oplus 1$ für c^* berechnen. Nun ist $(c^*, t^{**}) \neq (c^*, t^*)$ eine neue gültige Verschlüsselung von m_b und eine Anfrage an das Entschlüsselungsorakel liefert schliesslich m_b. Somit gewinnt $\mathcal{A}_{\text{cca}}$ das CCA-Spiel mit Wahrscheinlichkeit 1.

AUFGABE 3. CCA Sicherheit. (10 Punkte)
Es sei $F := \{F_k : \{0,1\}^{3n} \to \{0,1\}^{3n} | k \in \{0,1\}^n\}$ 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.

Lösungsvorschlag:

Sei $\mathcal{A}$ ein CCA-Angreifer auf Π mit Vorteil $\epsilon_{\mathcal{A},\Pi}(n)$, d.h.

$$\underset{b\in_R\{0,1\},k\leftarrow\mathsf{Gen}(1^n)}{\mathbf{Ws}}\left[\mathcal{A}(1^n,\mathsf{Enc}_k(m_b))=b\right]=\frac{1}{2}+\epsilon_{\mathcal{A},\Pi}(n)$$

und sei $q=q(n)=\mathsf{poly}(n)$ die Anzahl von Ver- und Entschlüsselungsanfragen von $\mathcal{A}$. Wir konstruieren nun einen Unterscheider $\mathcal{D}$ für F aus $\mathcal{A}$. Wir bezeichnen mit $\mathcal{O}$ und $\mathcal{O}^{-1}$ die Orakel, auf welche $\mathcal{D}$ zugreifen kann, d.h. $\mathcal{D}$ soll unterscheiden, ob $\mathcal{O}=F_k$ und $\mathcal{O}^{-1}=F_k^{-1}$ gilt oder ob $\mathcal{O}=P$ und $\mathcal{O}^{-1}=P^{-1}$ für eine *echte* Zufallspermutation ist. $\mathcal{D}$ funktioniert nun wie folgt.

- **Schlüsselerzeugung:** $\mathcal{D}$ wählt $k\in_R\{0,1\}^n$ und sendet 1^n an $\mathcal{A}$.
- **Ver- und Entschlüsselungsanfragen:** $\mathcal{A}$ stellt Ver- und Entschlüsselungsanfragen für $m_i\in\{0,1\}^n$ oder $c_j\in\{0,1\}^{3n}$. Im ersten Fall wählt $\mathcal{D}$ zufälliges $r_i\in\{0,1\}^n$ und sendet $c_i=\mathcal{O}(r_i||m_i||0^n)$ and $\mathcal{A}$, im zweiten Fall berechnet $\mathcal{D}$ zunächst $(x_j^1,x_j^2,x_j^3)=\mathcal{O}^{-1}(c_j)$ und falls $x_j^3=0^n$ gilt sendet $\mathcal{D}$ die Entschlüsselung x_j^2 and $\mathcal{A}$. Falls $x_j^3\neq 0^n$, so sendet $\mathcal{D}$ das Fehlersymbol $\perp$.
- **Challenge:** $\mathcal{A}$ sendert seine Challenge (m_1,m_2) und $\mathcal{D}$ schickt $c^*=\mathcal{O}(r^*||m_b||0^n)$ für $b\in_R\{0,1\}$ und $r^*\in\{0,1\}^n$.
- **Ver- und Entschlüsselungsanfragen:** Die zweite Phase von Ver- und Entschlüsselungsanfragen (mit der trivialen Einschränkung, dass $c_j\neq c^*$ für alle Anfragen c_j gelten muss) wird analog zur ersten realisiert.
- **Antwort:** $\mathcal{A}$ liefert schliesslich ein Bit b'. $\mathcal{D}$ gibt 1 aus genau dann, wenn $b=b'$ gilt.

Die Intuition der obigen Reduktion ist klar: Falls $(\mathcal{O},\mathcal{O}^{-1})=(F_k,F_k^{-1})$ gilt, so erhalten wir eine perfekt Simulation von $\mathcal{A}$'s CCA-Spiel. Andernfalls erhält $\mathcal{A}$ zufällige $3n$-Bitstrings, die keine Information über die zugrunde liegende Nachricht enthalten. Wir zeigen dies nun formal.

1. Fall: Sei $(\mathcal{O},\mathcal{O}^{-1})=(F_k,F_k^{-1})$, dann gilt

$$\mathbf{Ws}\left[\mathcal{D}^{\mathcal{O},\mathcal{O}^{-1}}(1^n)=1\right]=\mathbf{Ws}\left[\mathcal{D}^{F_k,F_k^{-1}}(1^n)=1\right]=\mathbf{Ws}\left[\mathcal{A}(1^n,c^*)=b\right]=\frac{1}{2}+\epsilon_{\mathcal{A},\Pi}(n)\ . \quad (1)$$

2. Fall: $(\mathcal{O},\mathcal{O}^{-1})=(P,P^{-1})$ für eine echte Zufallspermutation $P:\{0,1\}^{3n}\to\{0,1\}^{3n}$. Wir wollen nun zeigen, dass

$$\mathbf{Ws}\left[\mathcal{D}^{\mathcal{O},\mathcal{O}^{-1}}(1^n)=1\right]=\mathbf{Ws}\left[\mathcal{D}^{\mathcal{P},\mathcal{P}^{-1}}(1^n)=1\right]=\mathbf{Ws}\left[\mathcal{A}(1^n,c^*)=b\right]=\frac{1}{2}+\mathsf{negl}(n)$$

gilt. Wir bemerken zunächst, dass $\mathcal{A}$ nicht in der Lage ist, gültige Chiffretexte zu erzeugen, *ohne* diese zuvor bereits verschlüsselt haben zu lassen. Wir benutzen hierzu, dass wenn P eine echte Zufallspermutation ist, so ist auch P^{-1} eine echte Zufallspermutation. Ist nun $c\in\{0,1\}^{3n}$ ein von $\mathcal{A}$ erzeugter Chiffretext, so gilt für $(x_1,x_2,x_3)=\mathcal{O}^{-1}(c)$, dass $\mathbf{Ws}\left[x_3=0^n\right]=2^{-n}=\mathsf{negl}(n)$. Mit anderen Worten bedeutet dies, dass $\mathcal{A}$'s Entschlüsselungsorakel nutzlos wird (bis auf vernachlässigbare Wahrscheinlichkeit). Es bleibt zu zeigen, dass $\mathcal{A}$ mit einem Verschlüsselungsorakel sein CCA-Spiel nur mit Wahrscheinlichkeit $\frac{1}{2}+\mathsf{negl}(n)$

gewinnen kann. Dies kann man analog zum Beweis der CPA-Sicherheit des Verschlüsselungsverfahrens Π_B aus einer Pseudozufallsfunktion (siehe Vorlesung, Folie 73f) erreichen. Solange bei $\mathcal{A}$'s Verschlüsselungsanfragen *kein* $r_i = r^*$ benutzt wird, liefert der zugehörige Chiffretext c_i *keine* Information bzgl. c^*. Formal führt man hierzu analog zum Beweis von Π_B ein Ereignis Repeat ein mit $\mathsf{Repeat} = \mathsf{1}$ genau dann, wenn $r_i = r^*$ für mindestens ein $i \in [q]$ gilt. Nun folgt

$$\begin{aligned}\mathbf{Ws}\left[\mathcal{A}(1^n, c^*) = b\right] &= \mathbf{Ws}\left[\mathcal{A}(1^n, c^*) = b \wedge \mathsf{Repeat}\right] + \mathbf{Ws}\left[\mathcal{A}(1^n, c^*) = b \wedge \neg\mathsf{Repeat}\right] \qquad (2)\\ &\leq \mathbf{Ws}\left[\mathsf{Repeat}\right] + \mathbf{Ws}\left[\mathcal{A}(1^n, c^*) = b | \neg\mathsf{Repeat}\right] =\leq \frac{q(n)}{2^n} + \frac{1}{2} = \frac{1}{2} + \mathsf{negl}(n) \ .\end{aligned}$$

Zusammen liefern (1) und (2) schliesslich

$$\left|\mathbf{Ws}\left[\mathcal{D}^{F_k, F_k^{-1}}(1^n) = 1\right] - \mathbf{Ws}\left[\mathcal{D}^{P, P^{-1}}(1^n) = 1\right]\right| = \left|\epsilon_{\mathcal{A},\Pi}(n) - \mathsf{negl}(n)\right| \ .$$

Da F eine Familie von Pseudozufallspermutationen ist, folgt nun $\epsilon_{\mathcal{A},\Pi}(n) \leq \mathsf{negl}(n)$.