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

RUHR UNIVERSITÄT BOCHUM RUB

Hausübungen zur Vorlesung

Kryptographie 1

WS 2010/11

Blatt 5 / 13. Dezember 2010 / Abgabe 10. Januar, 16 Uhr, Kasten NA 02

AUFGABE 1. Kombiniere, kombiniere. (5 Punkte)
Nehmen Sie an, Ihnen stehen zwei MACs $\Pi^1 = (\mathsf{Gen}^1, \mathsf{Mac}^1, \mathsf{Vrfy}^1)$ und $\Pi^2 = (\mathsf{Gen}^2, \mathsf{Mac}^2, \mathsf{Vrfy}^2)$ zur Verfügung. Sie wissen, dass einer von beiden sicher ist (gemäß Folie 102), aber nicht welcher.

Kombinieren Sie beide MACs zu einem neuen, *sicheren* MAC $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$. Beweisen Sie die Sicherheit.

Hinweis: Erzeugen Sie ein Tag $t \leftarrow \mathsf{Mac}^1_{k_1}(m)||\mathsf{Mac}^2_{k_2}(m)$.

AUFGABE 2. MAC-Kandidat. (5 Punkte)
Sei $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ eine Pseudozufallsfunktion. Betrachten Sie den folgenden MAC $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ für Nachrichten fester Länge $m \in \{0,1\}^{2n}$.

$\mathsf{Gen}(1^n)$ gibt $k \in_R \{0,1\}^n$ aus.

$\mathsf{Mac}_k(m)$ berechnet für eine Nachricht $m = (m_0, m_1)$ mit $|m_0| = |m_1| = n$ den Tag

$$t = \langle F_k(m_0), F_k(F_k(m_1)) \rangle \ .$$

Geben Sie die Vrfy-Funktion an. Ist der MAC sicher?

AUFGABE 3. CBC-MAC. (5 Punkte)
Betrachten Sie folgende Modifikationen des CBC-MAC aus der Vorlesung (siehe Folie XX).

a) Beweisen Sie, dass der CBC-MAC aus der Vorlesung nicht sicher ist, wenn wir Nachrichten mit variabler Länge zulassen.

b) Anstelle eines fixen Initialisierungswertes $t_0 = 0^n$ wählen wir nun zufälliges $t_0 \in_R \{0,1\}^n$ und geben dieses am Ende zusätzlich mit aus, d.h. das Tag hat die Form $t = (t_0, t_\ell)$. Zeigen Sie, dass diese Konstruktion unsicher ist.

Geben Sie in beiden Fällen konkret an, wie Sie Fälschungen berechnen.

Der Begriff der CCA-Sicherheit aus der Vorlesung (siehe Folie 95ff) wird in der Literatur oft auch als *CCA2-Sicherheit* bezeichnet. Dies liegt daran, dass noch ein abgeschwächter Sicherheitsbegriff, die sogenannte *CCA1-Sicherheit*, existiert. Das Sicherheitsspiel zur CCA1-Sicherheit (siehe unten) verläuft identisch zum CCA2-Sicherheitsspiel, jedoch darf ein Angreifer *nach* Erhalt des Challenge Ciphertextes $c = \mathsf{Enc}_k(m_b)$ *keine* weiteren Entschlüsselungsanfragen mehr stellen. In der folgenden Aufgabe wollen wir zeigen, dass diese beiden Sicherheitsbegriffe tatsächlich unterschiedlich sind.

CCA1-Sicherheit

Sei $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ ein Verschlüsselungsverfahren. Wir definieren das Spiel $\mathsf{PrivK}^{cca1}_{\mathcal{A},\Pi}(n)$ wie folgt.

i) $k \leftarrow \mathsf{Gen}(1^n)$.

ii) $(m_0, m_1) \leftarrow \mathcal{A}^{\mathsf{Enc}_k(\_),\mathsf{Dec}_k(\_)}(1^n)$, d.h. $\mathcal{A}$ darf sowohl Ver- als auch Entschlüsselungsanfragen stellen.

iii) Wähle $b \in_R \{0,1\}$ und schicke $c \leftarrow \mathsf{Enc}_k(m_b)$ an $\mathcal{A}$.

iv) $b' \leftarrow \mathcal{A}^{\mathsf{Enc}_k(\_)}(c)$, d.h. $\mathcal{A}$ darf weitere Ver- aber *keine* Entschlüsselungsanfragen mehr stellen.

v) $\mathsf{PrivK}^{cca1}_{\mathcal{A},\Pi}(n) = \begin{cases} 1 & \text{falls } b = b' \\ 0 & \text{sonst} \end{cases}$.

Das Verfahren $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ besitzt *ununterscheidbare Chiffretexte gegenüber CCA1*, falls für alle ppt $\mathcal{A}$ gilt

$$\mathbf{Ws}\left[\mathsf{PrivK}^{cca1}_{\mathcal{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \mathsf{negl}(n) \ .$$

AUFGABE 4. CCA1 vs. CCA2. (5 Punkte)
Sei $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ ein CCA1-sicheres Verfahren. Konstruieren Sie hieraus ein Verfahren $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$, welches die CCA1-Sicherheit erbt, aber *nicht* CCA2-sicher ist. Es reicht, den Beweis der CCA1-Sicherheit zu skizzieren (sofern Ihre Konstruktion einfach genug ist, um dies zuzulassen). Geben Sie außerdem einen CCA2-Angreifer an.

Hinweis: Definiere $\mathsf{Enc}'_k(m) = \langle r, \mathsf{Enc}_k(m)\rangle$ für $r \in_R \{0,1\}$.