Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Eike Kiltz
Gottfried Herold

Hausübungen zur Vorlesung

Kryptographie I

WS 2011/2012

Blatt 5 / 16. Dezember 2011 / Abgabe **bis spätestens Montag, 9.01.2012 16:00 Uhr**

AUFGABE 1:

Sei F eine Pseudozufallsfunktion. Wir betrachten den folgenen MAC $\Pi = (\mathbf{Gen}, \mathbf{Mac}, \mathbf{Vrfy})$ für Nachrichten $m = (m_0, m_1) \in \{0,1\}^{2n}$:
Gen wählt $k \in_R \{0,1\}^n$ uniform.
$\mathbf{Mac}_k(m_0, m_1) := F_k(m_0) \,||\, F_k(m_1 \oplus F_k(m_0))$
$\mathbf{Vrfy}_k(t, m_0, m_1)$ prüft, ob $t = \mathbf{Mac}_k(m_0, m_1)$ gilt.

Zeigen, die dass dieser MAC *nicht* sicher ist[5 Punkte].
Bemerkung: Obige Definition ist CBC-MAC mit Ausgabe der Zwischenergebnisse für $l = 2$.

AUFGABE 2:

Seien $\Pi^1 = (\mathbf{Gen}^1, \mathbf{Mac}^1, \mathbf{Vrfy}^1)$ und $\Pi^2 = (\mathbf{Gen}^2, \mathbf{Mac}^2, \mathbf{Vrfy}^2)$ zwei MACs.
Wir nehmen an, dass mindestens einer von Π^1 oder Π^2 sicher ist, aber wir wissen nicht, welcher.
Konstruieren Sie aus diesen einen neuen sicheren MAC $\Pi = (\mathbf{Gen}, \mathbf{Mac}, \mathbf{Vrfy})$ und zeigen Sie, dass Π sicher ist, wenn mindestens einer von Π^1, Π^2 dies ist.
[5 Punkte]

AUFGABE 3:

Sei $\Pi = (\mathbf{Gen}, \mathbf{Mac}, \mathbf{Vrfy})$ zunächst ein beliebiger MAC. Betrachten Sie das Spiel Mac-Forge$'_{A,\Pi}(n)$ für einen Algorithmus A:

MAC-Forge$'_{A,\Pi}(n)$		A
$k \leftarrow_\$ \mathbf{Gen}(1^n)$	$\xrightarrow{1^n}$	
		$m_i \in \mathcal{M}$, $i = 1, \ldots, q$
$t_i = \mathbf{Mac}_k(m_i) \forall i$	$\xleftarrow{m_i}$	
	$\xrightarrow{t_i}$	
Ausgabe 1, falls $\mathbf{Vrfy}(m,t) = 1$	$\xleftarrow{(m,t)}$	Berechne (m,t), wobei $(m,t) \neq (m_i, t_i) \forall i$.
Ausgabe 0, falls $\mathbf{Vrfy}(m,t) \neq 1$		

Der einzige Unterschied zum normalen MAC-Forge-Spiel ist, dass lediglich $(m,t) \neq (m_i, t_i)$ gelten muss anstatt $m \neq m_i$. Das bedeutet, dass es eine gültige Fälschung darstellt, zu einer bereits angefragten Nachricht einen *neuen* (d.h. anderen als vom Spiel erhaltenen) gültigen Tag zu berechnen.

Wir nennen Π stark sicher, wenn $\mathbf{Ws}[\text{Mac-Forge}'_{A,\Pi}(n) = 1] = \text{negl}(n)$ für alle ppt Algorithmen A.

Sei nun $\Pi = (\mathbf{Gen}, \mathbf{Mac}, \mathbf{Vrfy})$ ein sicherer (nach der Definition der Vorlesung) MAC. Konstruieren Sie daraus einen neuen MAC $\Pi' = (\mathbf{Gen}', \mathbf{Mac}', \mathbf{Vrfy}')$, der sicher ist, aber nicht stark sicher. Zeigen Sie, dass Ihre Konstruktion dies erfüllt, d.h.:[7 Punkte]

- Π' ist sicher nach der Defintion aus der Vorlesung, wenn Π dies ist.
- Π' ist nicht stark sicher.

Hinweis:
Ergänzen Sie **Mac** um ein Bit.

AUFGABE 4:

Sei F eine Pseudozufallsfunktion. Betrachten Sie den folgenden MAC $\Pi = (\mathbf{Gen}, \mathbf{Mac}, \mathbf{Vrfy})$ mit Nachrichtenraum $\mathcal{M} = \{0,1\}^{\frac{n}{2}}$:

Gen wählt $k \in_R \{0,1\}^n$ uniform.
$\mathbf{Mac}_k(m)$ wählt $r \in_R \{0,1\}^n$ uniform und gibt $(r, F_k(r) \oplus F_k(0^{\frac{n}{2}} \,||\, m))$ aus.
$\mathbf{Vrfy}_k(m,t)$ testet ob für $t = (r, t_1)$ gilt, dass $t_1 = F_k(r) \oplus F_k(0^{\frac{n}{2}} \,||\, m)$ erfüllt ist.

Zeigen Sie, dass Π *nicht* sicher ist [3 Punkte].

Hinweis:
Beachten Sie, dass Sie r für die Fälschung beliebig wählen dürfen.