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

Hausübungen zur Vorlesung

Kryptographie I

WS 2011/2012

Blatt 4 / 22. November 2011 / Abgabe **bis spätestens Montag, 5.12.2011 16:00 Uhr**

AUFGABE 1:

Sei $G : \{0,1\}^n \to \{0,1\}^{l(n)}$ ein PRG.
Für $m = \text{poly}(n)$, betrachten wir $G^{(m)} : \{0,1\}^{m \cdot n} \to \{0,1\}^{m \cdot l(n)}$, definiert durch $G^{(m)}(s_1 \,||\, s_2 \,||\, \cdots \,||\, s_m) = G(s_1) \,||\, G(s_2) \,||\, \cdots \,||\, G(s_m)$, d.h. $G^{(m)}$ entspricht der parallelen Ausführung von m Kopien von G mit unabhängigen Seeds.

Zeigen Sie: $G^{(m)}$ ist ein PRG. [5 Punkte]

Hinweis: Ersetzen Sie per Hybridargument die einzelnen $G(s_i)$ nacheinander durch uniforme Bits.

AUFGABE 2:

Zeigen Sie, dass jede Pseudozufallspermutation eine Pseudozufallsfunktion ist. [5 Punkte]

Hinweis: Zeigen Sie dazu, dass ein ppt. Unterscheider (der sein Orakel nur an $q(n) = \text{poly}(n)$ vielen Stellen auswerten kann) eine zufällige Funktion nicht von einer zufälligen Permutation unterscheiden kann, d.h. für alle ppt. Unterscheider D gilt:

$$|\mathbf{Ws}[D^{f(.)}(1^n) = 1] - \mathbf{Ws}[D^{g(.)}(1^n) = 1]| = \text{negl}(n)$$

für $f \in_R \text{Func}_n, g \in_R \text{Perm}_n$ uniform zufällige Funktion bzw. Permutation.

AUFGABE 3:

Sei $F : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n, (k,x) \mapsto F_k(x)$ eine längenerhaltende schlüsselabhängige Funktion.

Wir konstruieren eine neue schlüsselabhängige Funktion $F' : \{0,1\}^m \times \{0,1\}^{n-1} \to \{0,1\}^{2n}$ mittels

$$F'_k(x) := F_k(x \,||\, 0) \,||\, F_k(x \,||\, 1)$$

Zeigen Sie: F' ist eine Pseudozufallsfunktion[1] genau dann wenn F eine Pseudozufallsfunktion ist. [5 Punkte]

AUFGABE 4:

Sei F eine Pseudozufallsfunktion. Wir betrachten folgende Modifikation des CBC-Modus: Der 1. Initialisierungsvektor $IV^1 \in_R \{0,1\}^n$ wird uniform zufällig gewählt. Von da ab wird der Initialisierungsvektor IV^i für die i-te Verschlüsselung (CPA-Anfragen oder Verschlüsselung des Challenge-Ciphertexts m_b) als $IV^i = IV^1 + (i-1) \bmod 2^n$ gewählt, d.h. jedes mal um 1 erhöht. (Wir identifizieren hierbei $\{0,1\}^n$ mit $\mathbb{Z}_{2^n}$)

Zeigen Sie, dass das resultierende Verfahren *nicht* CPA-sicher ist. [5 Punkte]

[1] F' ist nicht längenerhaltend, was aber für die Definition von Pseudozufallsfunktion nicht wesentlich ist