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

Hausübungen zur Vorlesung

Kryptographie II

SS 2012

Blatt 3 / 10. Mai 2012 / Abgabe **bis spätestens Mittwoch, 23.05.2012 10:00 Uhr**

AUFGABE 1:

Sei $\Pi_{\mathrm{f}} = (\mathrm{Gen}, \mathrm{Samp}, \mathrm{f})$ eine Familie von Einwegfunktionen, hc deterministischer pt Algorithmus mit Ausgabe eines einzelnen Bits $\mathrm{hc}(x)$ für $x \in D$.
Zeigen Sie:[4 Punkte]

hc ist Hardcore-Prädikat für Π_{f} genau dann, wenn die Verteilungen $(1^n, I, f(x), \mathrm{hc}(x))$ und $(1^n, I, f(x), u)$ durch ppt Algorithmen ununterscheidbar sind, wobei $I \leftarrow \mathbf{Gen}(1^n), x \leftarrow \mathrm{Samp}(I)$ und $u \in \{0,1\}$ uniform. Dies bedeutet, dass für alle ppt A gilt:
$|\mathrm{Ws}[A(1^n, I, f(x), \mathrm{hc}(x)) = 1] - \mathrm{Ws}[A(1^n, I, f(x), u)] = 1| = \mathrm{negl}(n)$

AUFGABE 2:

Geben Sie eine längenerhaltende (durch det. pt. Alg berechenbare) Funktion $f : \{0,1\}^* \to \{0,1\}^*$ und ein Hardcore-Prädikat hc für f an, so dass f *keine* Einwegfunktion ist.
Zeigen Sie, dass Ihre Konstruktion die geforderten Eingenschaften erfüllt. [4 Punkte]

Bemerkungen/Hinweise: f muss hierbei keine Familie sein.
Für Permutationen impliziert die Existenz eines Hardcoreprädikats die Einwegeigenschaft. Insbesondere sollte Ihre Konstruktion daher nicht bijektiv sein.
Für das Hardcore-Prädikat bietet sich an, f und hc so zu wählen, dass $f(x)$ und $\mathrm{hc}(x)$ (wsk-theoretisch) unabhängig sind.

AUFGABE 3:

Sei $f : \{0,1\}^* \to \{0,1\}^*$ längenerhaltende Einwegfunktion.
Zeigen Sie, dass dann auch

$$g(x) = (f(x), f(f(x)))$$

eine Einwegfunktion ist. [3 Punkte]

bitte wenden

AUFGABE 4:

Seien $f : \{0,1\}^* \to \{0,1\}^*$ und $g : \{0,1\}^* \to \{0,1\}^*$ zwei längenerhaltende, durch det. pt. Alg. berechenbare *Permutationen*. Sei weiterhin *mindestens eine* der Permutationen f, g eine Einwegpermutation. Zeigen Sie dass dann

$$h(x) = f(g(x))$$

eine Einwegpermutation ist. [5 Punkte]

AUFGABE 5:

(Bonusaufgabe) [4 Bonuspunkte]
Sei f eine längenerhaltende Einwegfunktion. Zeigen Sie, dass dann nicht notwendigerweise gilt, dass $f(f(x))$ eine Einwegfunktion ist.

Konstruieren Sie dazu ausgehend von einer beliebigen längenerhaltenden Einwegfunktion f eine neue längenerhaltende Einwegfuntion f', für die $f'(f'(x))$ keine Einwegfunktion ist.