Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Stefan Hoffmann, Ilya Ozerov

Hausübungen zur Vorlesung

Kryptographie

WS 2013/14

Blatt 12 / 20. Januar 2014

Abgabe: 28. Januar 2014, 14.00 Uhr (vor der Vorlesung), Kasten NA/02

AUFGABE 1 (10 Punkte)**:**

Sei $f : \{0,1\}^{2n} \to \{0,1\}^{2n}$ eine Einwegfunktion. Zeigen Sie, dass dann im Allgemeinen die Funktion $f' : \{0,1\}^{2n} \to \{0,1\}^{2n}$ definiert durch $f'(x) := f(x) \oplus x$ keine Einwegfunktion ist. Gehen Sie wie folgt vor:

(a) Sei $g : \{0,1\}^n \to \{0,1\}^n$ eine Einwegfunktion. Zeigen Sie, dass dann auch $f : \{0,1\}^{2n} \to \{0,1\}^{2n}$ definiert durch

$$f(x) = f(x_1, x_2) := (g(x_1) \oplus x_2, x_2)$$

eine Einwegfunktion ist. Wir teilen die Eingabe $x \in \{0,1\}^{2n}$ in zwei Hälften x_1 und x_2 mit $x_1, x_2 \in \{0,1\}^n$ auf.

Hinweis: Beim Nachweis der Einwegeigenschaft kann es hilfreich sein, zunächst die Mengengleichheit $f^{-1}(a,b) = g^{-1}(a \oplus b) \times \{b\}$ zu zeigen. Hierbei bezeichnet $f^{-1}(a,b) := \{(x_1, x_2) \in \{0,1\}^{2n} \mid f(x_1, x_2) = (a,b)\}$ das *Urbild* von (a,b) unter f.

(b) Benutzen Sie das in (a) konstruierte f und betrachten Sie das entsprechende f'. Zeigen Sie, dass dieses f' keine Einwegfunktion sein kann.

Bitte wenden!

AUFGABE 2 (5 Punkte)**:**

Sei $\Pi_f = (\mathsf{Gen}, \mathsf{Samp}, f_I, \mathsf{Inv})$ eine Familie von Trapdoor-Einwegpermutationen und $\mathsf{dh} : \{0,1\}^n \to \{0,1\}^2$ ein Doppelhardcoreprädikat für Π_f (siehe Präsenzübung 12, Aufgabe 3). Konstruieren Sie aus Π_f und dh analog zur Vorlesung (Folie 65) ein asymmetrisches Verschlüsselungsverfahren $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ für Nachrichten $m \in \{0,1\}^2$.

Zeigen Sie die Korrektheit und die CPA-Sicherheit Ihres Verfahrens.

Hinweis: Raten Sie wie im Beweis auf Folie 68 das Doppelhardcoreprädikat mit $z \in_R \{0,1\}^2$. Betrachten Sie dann in der Reduktion die Ereignisse $\mathsf{GOOD} := (z = \mathsf{dh}(x) \wedge b = b')$ und $\mathsf{OKAY} := (z = \mathsf{dh}(x) \oplus m_0 \oplus m_1 \wedge b \neq b')$. Das Ereignis GOOD beschreibt also die Tatsache, dass dh richtig geraten wurde und der Angreifer korrekt antwortet, während OKAY das Ereignis beschreibt, dass z einen speziellen Wert annimmt und der Angreifer zudem mit seiner Antwort falsch liegt. Betrachten Sie oBdA nur Angreifer, die $m_0 \neq m_1$ wählen. Schätzen Sie schließlich $\mathsf{Ws}[d' = \mathsf{dh}(x)] \geq \mathsf{Ws}[d' = \mathsf{dh}(x) \wedge \mathsf{GOOD}] + \mathsf{Ws}[d' = \mathsf{dh}(x) \wedge \mathsf{OKAY}]$ ab. Dabei entspricht d' dem Wert, den $\mathcal{A}'$ zum Schluss ausgibt.

AUFGABE 3 (5 Punkte)**:**

Betrachten Sie folgende modifizierte Version der *quadratischen Residuositätsannahme* (siehe Folie 86), in welcher der Unterscheider $y \in_R \mathcal{QNR}_N$ anstelle von $y \in_R \mathcal{QNR}_N^{+1}$ erhält.

Das Unterscheiden quadratischer Reste ist hart bzgl. $\mathsf{GenModulus}(1^n)$*, falls für alle ppt-Unterscheider* $\mathcal{D}$ *gilt*

$$|\mathsf{Ws}_{x \in_R \mathcal{QR}_N}[\mathcal{D}(1^n, N, x) = 1] - \mathsf{Ws}_{y \in_R \mathcal{QNR}_N}[\mathcal{D}(1^n, N, y) = 1]| \leq \mathsf{negl}(n).$$

Zeigen Sie, dass die modifizierte Annahme nie gelten kann, indem Sie einen Unterscheider $\mathcal{D}$ konstruieren, der die beiden Verteilungen mit Wahrscheinlichkeit $\geq 2/3$ unterscheidet.