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

Präsenzübungen zur Vorlesung

Kryptographie I

WS 2012/13

Blatt 2 / 29./31. Oktober 2012

AUFGABE 1:

Entscheiden Sie, welche der folgenden Funktionen vernachlässigbar sind. Begründen Sie.

$$(a)\ 0.80^n, \quad (b)\ \frac{1}{2^{80}n}, \quad (c)\ \frac{1}{2^{80n}}, \quad (d)\ 2^{-\log_2(n^{80})}.$$

In den nächsten beiden Aufgaben (und in der Hausaufgabe) wollen wir die Äquivalenz dreier Definitionen von KPA-Sicherheit zeigen. Die erste Definition ist bekannt aus der Vorlesung:

Definition 1. Ein Verschlüsselungsschema $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ besitzt *ununterscheidbare Chiffretexte gegenüber KPA*, falls für alle ppt Angreifer $\mathcal{A}$ gilt

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

Alternativ kann man definieren, dass der Betrag des *Vorteils* jedes Angreifers vernachlässigbar sein muss:

Definition 2. Ein Verschlüsselungsschema $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ besitzt *ununterscheidbare Chiffretexte gegenüber KPA*, falls für alle ppt Angreifer $\mathcal{A}$ gilt

$$\left|\mathsf{Ws}[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1] - \frac{1}{2}\right| \leq \mathsf{negl}(n)$$

Für die dritte Definition müssen wir das KPA-Spiel leicht modifizieren. Wir definieren dazu $\mathsf{PrivK}^{\mathsf{eav},b}_{\mathcal{A},\Pi}(n)$ für $b \in \{0,1\}$ analog zum KPA-Spiel, mit dem einzigen Unterschied, dass die ausgewählte Nachricht, also das Bit b, nicht zufällig gewählt, sondern von außen fixiert wird. Das Ziel des Angreifers $\mathcal{A}$ ist nun zu entscheiden, in welchem Spiel $b = 0$ oder $b = 1$ er sich befindet. Die Ausgabe des Angreifers $\mathcal{A}$ wird im jeweiligen Spiel mit $\mathsf{out}(\mathsf{PrivK}^{\mathsf{eav},b}_{\mathcal{A},\Pi}(n))$ bezeichnet.

Definition 3. Ein Verschlüsselungsschema $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ besitzt *ununterscheidbare Chiffretexte gegenüber KPA*, falls für alle ppt Angreifer $\mathcal{A}$ gilt

$$\left|\mathsf{Ws}[\mathsf{out}(\mathsf{PrivK}^{\mathsf{eav},1}_{\mathcal{A},\Pi}(n)) = 1] - \mathsf{Ws}[\mathsf{out}(\mathsf{PrivK}^{\mathsf{eav},0}_{\mathcal{A},\Pi}(n)) = 1]\right| \leq \mathsf{negl}(n)$$

AUFGABE 2:

Zeigen Sie, dass die erste Definition die zweite Definition impliziert.

Hinweis: Führen Sie eine Fallunterscheidung durch und betrachten Sie im zweiten Fall den Angreifer $\bar{\mathcal{A}}$, der das Gegenteil von $\mathcal{A}$ ausgibt.

AUFGABE 3:

Zeigen Sie:

$$\mathsf{Ws}[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1] = \frac{1}{2} + \frac{1}{2} \cdot \left(\mathsf{Ws}[\mathsf{out}(\mathsf{PrivK}^{\mathsf{eav},1}_{\mathcal{A},\Pi}(n)) = 1] - \mathsf{Ws}[\mathsf{out}(\mathsf{PrivK}^{\mathsf{eav},0}_{\mathcal{A},\Pi}(n)) = 1]\right)$$

AUFGABE 4:

(a) Sei $G : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ ein Pseudozufallsgenerator. Sei $\bar{G} : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ definiert als $\bar{G}(s) := G(s) \oplus 1^{\ell(n)}$, d.h. wir benutzen die Ausgabe von G und invertieren alle Bits. Zeigen Sie, dass auch $\bar{G}$ ein Pseudozufallsgenerator ist.

(b) Seien G_1, G_2 zwei verschiedene Pseudozufallsgeneratoren. Wir definieren nun G' als $G'(s) := (G_1(s), G_2(s))$, d.h. die Ausgaben der einzelnen Generatoren werden aneinandergehangen. Zeigen Sie, dass G' im Allgemeinen kein Pseudozufallsgenerator ist!

Hinweise: Für (a) sollten Sie zeigen, dass Sie aus einem Unterscheider für $\bar{G}$ einen Unterscheider für G konstruieren können. Für (b) sollten Sie Teil (a) benutzen, um ein Gegenbeispiel zu finden. Geben Sie für Ihr Gegenbeispiel einen Unterscheider an und zeigen Sie, dass dieser nicht-vernachlässigbare Erfolgswahrscheinlichkeit hat.